КРИТЕРІЇ ОЦІНКИ СТАНУ ДОТРИМАННЯ ПРАВ ЛЮДИНИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

2025

Лабораторія цифрової безпеки

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

ПРО КРИТЕРІЇ

Лабораторія цифрової безпеки розробила критерії оцінки стану дотримання прав людини в цифровому середовищі з метою системного аналізу виконання Україною міжнародних зобов'язань в умовах цифрової трансформації, євроінтеграції та воєнного стану. Критерії базується на положеннях ключових міжнародних актів, таких як Конвенція про захист прав людини і основоположних свобод (ЄКПЛ), Міжнародний пакт про громадянські і політичні права (МПГПП), акти права Європейського Союзу, включаючи Загальний регламент захисту даних (GDPR), Акт про цифрові послуги (DSA), Акт про штучний інтелект (AI Act), Європейський акт про свободу медіа та відповідні рекомендації Ради Європи, практики Європейського суду з прав людини та інших джерелах. Документ включає п'ять основних блоків: доступ до Інтернету, свобода вираження поглядів онлайн та свобода медіа, захист персональних даних і приватності, вплив технологій штучного інтелекту на права людини, а також цифровий вимір права на вільні вибори. У межах кожного блоку визначено чіткі критерії оцінки, що охоплюють як наявність правових гарантій, так і практичне забезпечення прав. Критерії також враховують обставини воєнного стану, та дають можливість відрізняти законні тимчасові обмеження прав від порушень міжнародних стандартів. Застосування цього інструменту допомагає виявляти прогалини в українському законодавстві, неузгодженість із європейськими нормами та конкретні випадки порушень прав у цифровому середовищі. Аналіз відповідно до розроблених критеріїв допоможе формулювати рекомендації для органів влади, парламенту, бізнесу та громадянського суспільства – зокрема, щодо реформ, необхідних для євроінтеграції та виконання вимог глав 23 (Судова влада та основоположні права) і 10 (Цифрова трансформація та медіа) переговорного процесу з ЄС. Крім того, документ сприяє підвищенню прозорості та підзвітності держави перед громадянами і міжнародними партнерами. У подальшому Лабораторія цифрової безпеки розширюватиме сфери аналізу, щоб охопити також вплив цифровізації на інші основоположні права людини.

Критерії підготовлено в рамках проєкту «Права людини у цифровому вимірі: дотримання міжнародних зобов'язань та план дій на шляху до ЄС» за підтримки Міжнародного фонду «Відродження». Документ представляє позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження».

Лабораторія цифрової безпеки (Цифролаба) *- українська неурядова організація, що допомагає незалежним медіа, журналістам, активістам та громадянському суспільству посилювати власну цифрову безпеку. Цифролаба також працює над впровадженням стандартів прав людини в цифровій сфері через напрацювання аналітичних матеріалів, долучення до законотворчих процесів та адвокаційних кампаній в Україні та світі.*

Сайт: https://dslua.org/
E-mail: dslua@dslua.org
ФБ: https://www.facebook.com/dslua

Міжнародний фонд «Відродження» *– одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів на суму понад 350 мільйонів доларів США.*

Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

ЗМІСТ

1. ДОСТУП ДО ІНТЕРНЕТУ ЯК ОСНОВА ДЛЯ РЕАЛІЗАЦІЇ ПРАВ ЛЮДИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ	
1.1. Забезпечення загального доступу до мережі Інтернет	
Інтернет доступний без перешкод та за прийнятну плату для всіх осіб без дискримінації.	Конвенція про захист прав людини і основоположних свобод (стаття 10); Міжнародний пакт про громадянські і політичні права (стаття 19); European Electronic Communications Code (Article 84); Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (para. 2.1.1).
1.2. Спеціальні заходи гарантування доступу до мережі Інтернет для вразливих соціальних груп	
Держава сприяє в доступі до інтернету через спеціальні точки в місцях надання публічних послуг, навчальних закладах, а також приватними компаніями. Держава вживає розумних заходів для забезпечення доступу до інтернету вразливим групам населення, у віддалених та сільських районах, а також людям з інвалідністю.	European Electronic Communications Code (Article 85); Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (paras. 2.1.2-3).
1.3. Гарантування умов для вільного доступу до якісних послуг інтернету	
Користувачі мають право вільно обирати провайдерів послуг доступу до інтернету на плюралістичному ринку наявних послуг.	European Electronic Communications Code (Article 12); Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.
1.4. Законність та обґрунтованість обмежень надання послуг доступу до мережі Інтернет	
Відсутні загальні відключення інтернету, крім виключних ситуацій, пов'язаних з запровадженням правового режиму надзвичайного стану чи інших заходів, спрямованих на захист інтересів територіальної цілісності та національної безпеки, за умови їх передбачуваності національним законодавством. Заходи щодо обмеження доступу до інтернету мають застосовуватися під наглядом суду або незалежного адміністративного органу, за умови, що цей захід є найменш обтяжливим для досягнення відповідної легітимної цілі. Необхідність продовження такого заходу має постійно	Конвенція про захист прав людини і основоположних свобод (стаття 10); Міжнародний пакт про громадянські і політичні права (стаття 19); Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (para. 2.1.7).

переглядатися судом чи іншим незалежним органом. Особа, чиє право обмежене, має право на перегляд такого рішення в суді, відповідно до вимог щодо права на справедливий судовий розгляд.		
1.5. Доступ до інтернету в умовах воєнного стану		
Загальні відключення інтернету допускаються лише у виключних ситуаціях, пов'язаних з необхідністю проведення військових операцій та інших заходів з захисту суверенітету. Такі заходи запроваджуються виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим зобов'язанням згідно з міжнародним правом, є необхідними та пропорційними. Будь-які вжиті заходи мають бути переглянуті та скасовані після припинення дії правового режиму воєнного стану.		Конвенція про захист прав людини і основоположних свобод (статті 10, 15); Міжнародний пакт про громадянські і політичні права (статті 4, 19).
2. СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ У ЦИФРОВОМУ СЕРЕДОВИЩІ		
2.1. Свобода отримувати та поширювати інформацію онлайн		
2.1.1. Законодавчі гарантії свободи отримувати та поширювати інформацію онлайн	Національне законодавство належно гарантує свободу вираження поглядів для кожного користувача цифрового середовища. Принципи обмеження свободи вираження поглядів, закріплені національним законодавством, відповідають міжнародному праву. Користувачі мають право оскаржувати рішення, що обмежують їх право на свободу вираження поглядів, у компетентних національних органах.	Конвенція про захист прав людини і основоположних свобод (стаття 10); Міжнародний пакт про громадянські і політичні права (стаття 19).
2.1.2. Законні та обґрунтовані підстави блокування Інтернет-ресурсів та фільтрування онлайн-контенту	Категорії протиправного контенту, що можуть спричиняти обмеження доступу до онлайн-контенту або сайтів, за допомогою яких він поширюється, мають бути чітко встановлені законодавством.	ECtHR, OOO Flavus v Russia (paras. 32-35).
	Будь-які заходи, що вживаються судами або незалежними державними органами для блокування, фільтрування або видалення онлайн-контенту, або будь-який запит з їх боку здійснювати такі дії супроводжується дотриманням умов щодо законності, легітимності і пропорційності обмежень (необхідності у демократичному суспільстві). Блокування ресурсу може застосовуватися лише у випадку, коли застосування інших заходів не є ефективним для забезпечення визначеного легітимного інтересу.	Конвенція про захист прав людини і основоположних свобод (стаття 10); Міжнародний пакт про громадянські і політичні права (стаття 19); Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (paras. 2.2.1-2); ECtHR, Cengiz and Others v Turkey, (paras. 60-65); ECtHR, OOO Flavus v Russia (para. 38).

	При цьому, оцінка протиправності контенту та оцінка правомірності блокування внаслідок поширення на платформі такого контенту мають бути відмінними.	
	У разі застосування блокування сайтів, відповідні державні органи мають дотримуватися гарантій належної процедури, зокрема ініціювати періодичний перегляд застосованих заходів на предмет необхідності їх застосування.	Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, (para. 1 (f)).
	Правила фільтрування та видалення онлайн-контенту під час воєнного стану мають бути чітко встановлені законодавством, бути необхідними та пропорційними та спрямовуватися на досягнення легітимного інтересу захисту національної безпеки. Органи, що здійснюють таке фільтрування чи видалення, мають належно оприлюднювати рішення про обмеження доступу до контенту та зазначати причини його ухвалення, з подальшим переглядом після закінчення правового режиму воєнного стану.	Конвенція про захист прав людини і основоположних свобод (статті 10, 15); Міжнародний пакт про громадянські і політичні права (статті 4, 19).
2.1.3. Обмеження свободи вираження поглядів, запроваджені в інтересах національної безпеки, територіальної цілісності, громадської безпеки, для запобігання заворушенням чи злочинам	Законодавство щодо захисту національної безпеки, територіальної цілісності, громадської безпеки, запобігання заворушенням чи злочинам не застосовуються у спосіб, який обмежує публічні дискусії з питань суспільного інтересу. Таке законодавство накладає обмеження на свободу вираження поглядів тільки у відповідь на нагальні суспільні потреби, що повинні визначатися якомога вузько, та передбачати співмірні санкції. Держава може покладатися на мету захисту національної безпеки лише у випадках, коли законодавче обмеження на свободу вираження поглядів має справжньою метою та наочним наслідком захист існування країни або її територіальної цілісності від застосування чи погрози застосування сили, або захист її здатності реагувати на застосування чи погрозу застосування сили, або із зовнішнього, як-от військова загроза, або із внутрішнього джерела, як-от підбурювання до насильницького повалення уряду.	Конвенція про захист прав людини і основоположних свобод (стаття 10); Міжнародний пакт про громадянські і політичні права (стаття 19); Johannesburg Principles on National Security, Freedom of Expression and Access to Information (prin 1-2).

2.1.4. Обмеження свободи вираження поглядів, пов'язані з захистом репутації і прав інших осіб	Преса відіграє суттєву роль у демократичному суспільстві. І хоча вона не може переступати певні межі, зокрема щодо репутації та прав інших осіб, тим не менш, її обов'язком є передавати у спосіб, сумісний із її обов'язками та відповідальністю, інформацію та ідеї з усіх питань загального інтересу. Межа допустимої критики щодо політика, який виступає у своїй публічній якості, є ширшою ніж щодо приватної особи. Право на захист репутації поширюється і на політиків, навіть коли вони виступають не як політики, проте вимоги такого захисту мають бути збалансовані з інтересами суспільства до відкритої дискусії з політичних питань. Національне законодавство має розрізняти факти та оціночні судження. Вимога довести правдивість оціночних суджень є нездійсненною і порушує свободу висловлення думки як таку, що є фундаментальною частиною свободи вираження поглядів. Однак навіть якщо висловлення є оціночним судженням, пропорційність втручання має залежати від того, чи існує достатній фактичний базис для оспорюваного висловлювання. Залежно від обставин конкретної справи, висловлювання, яке є оціночним судженням, може бути перебільшеним за відсутності будь-якого фактичного підґрунтя	ECtHR, Українська Прес-Група" проти України (пара. 38-42).
	Підходи, які регулюють відтворення матеріалу з друкованих засобів масової інформації та Інтернету, можуть відрізнятися та коригуватися з урахуванням особливостей технології. Беручи до уваги важливість Інтернету для загального здійснення права на свободу вираження, відсутність на національному рівні достатньої законодавчої бази, яка б дозволяла журналістам використовувати отриману з інтернету інформацію без остраху наразитися на санкції, серйозно перешкоджає пресі відігравати свою роль «сторожового пса суспільства».	ECtHR, «Редакція газети «Правоє дело» та Штекель проти України» (пара. 63-64).

	Судові провадження проти участі громадськості (SLAPP) можуть негативно вплинути на довіру та репутацію осіб, які беруть участь у громадському житті, і можуть виснажити їхні фінансові та інші ресурси. Необхідна надійна система гарантій та захисту, щоб журналісти-розслідувачі могли виконувати свою вирішальну роль як наглядачів за питаннями, що становлять суспільний інтерес, не боячись покарання за пошук правди та інформування громадськості. Інші важливі учасники публічних дебатів, такі як правозахисники, науковці, дослідники чи митці, також заслуговують на належний захист, оскільки вони також можуть стати мішенню для SLAPP. Держави забезпечують, щоб у випадках порушення судових проваджень проти фізичних або юридичних осіб, у зв'язку з їхньою участю в громадській діяльності, національне законодавство містило гарантії захисту, зокрема, можливість вимагати дострокового відхилення явно необґрунтованих позовів, право на відшкодування витрат, пов'язаних із участю у відповідному провадженні (наприклад, обґрунтовані витрати на правову допомогу та за заподіяні збитки), вимоги щодо прискореного судового розгляду та ін. Держави мають вживати заходи моніторингу та оприлюднення інформації щодо судових справ ініційованих проти осіб, у зв'язку з їх громадською участю, а також гарантувати належний доступ до інформації про доступні способи захисту та джерела підтримки.	Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation'); Commission Recommendation (EU) 2022/758 of 27 April 2022 on protecting journalists and human rights defenders who engage in public participation from manifestly unfounded or abusive court proceedings ('Strategic lawsuits against public participation') Recommendation CM/Rec(2024)2 of the Committee of Ministers to member States on countering the use of strategic lawsuits against public participation (SLAPPs).
2.1.5. Обмеження свободи вираження поглядів для захисту моралі та охорони здоров'я	Свобода вираження поглядів стосується не тільки «інформації» чи «ідей», які сприймаються зі схваленням чи розглядаються як необразливі або нейтральні, але й тих, які можуть ображати, шокувати чи непокоїти. Саме такими є вимоги плюралізму, толерантності та широти поглядів, без яких немає «демократичного суспільства».	ЄСПЛ, Сінькова проти України (para. 104).
	Погляди на вимоги моралі варіюються залежно від часу і місця. Завдяки своєму безпосередньому і безперервному контакту зі своїми країнами державні органи знаходяться в кращому становищі, ніж міжнародний судовий орган, щоб висловити думку про точний зміст цих вимог, а також про необхідність обмежень або покарань, спрямованих на їх дотримання. Попри те, що мораль є чутливою категорією, яку національні органи можуть оцінити краще, ніж міжнародний судовий орган, національні органи не мають необмеженої дискреції щодо таких питань. Під час аналізу обмежень	ECtHR, Müller and Others v. Switzerland (para. 35). ECtHR, Open Door and Dublin Well Woman v. Ireland (paras. 67-77).

	необхідно застосовувати принцип пропорційності, що передбачає важливим підґрунтям для захисту моралі ситуації, в якій йдеться про захист інтересів дітей та молоді.	
	Держави-члени ЄС повинні забезпечити свободу прийому і не обмежувати ретрансляцію на своїй території аудіовізуальних медіа-послуг з інших держав-членів з причин, які підпадають під сфери, що координуються Директивою. Держави-члени можуть вживати заходів для відступу стосовно певної послуги, якщо такі заходи є, зокрема, необхідними для захисту неповнолітніх та охорони здоров'я населення.	Audiovisual Media Services Directive (Article 3).
	Держава забезпечує, щоб аудіовізуальні комерційні повідомлення, які надають провайдери медіапослуг, які перебувають під її юрисдикцією, не принижували людську гідність; не містили будь-яку дискримінацію на основі статі, раси або етнічного походження, громадянства, релігії або віросповідання, інвалідності, віку або сексуальної орієнтації; не заохочували поведінку, яка завдає шкоди здоров'ю та безпеці чи охороні довкілля. Всі види аудіовізуальних комерційних повідомлень про сигарети та інші тютюнові вироби, а також про електронні сигарети та заправні контейнери повинні бути заборонені, а аудіовізуальні комерційні повідомлення про алкогольні напої не повинні бути спеціально призначені для неповнолітніх та не повинні сприяти надмірному вживанню таких напоїв. Держави повинні заохочувати використання співрегулювання та сприяти впровадженню саморегулювання стосовно неналежних аудіовізуальних комерційних повідомлень про алкогольні напої. Такі кодекси повинні бути спрямовані на ефективне зниження впливу на неповнолітніх аудіовізуальних комерційних повідомлень про алкогольні напої. Аудіовізуальні комерційні повідомлення про лікарські засоби та медичне лікування, які доступні тільки за призначенням лікаря, повинні бути заборонені. Аудіовізуальні комерційні повідомлення не повинні завдавати фізичної, психічної або моральної шкоди неповнолітнім; також, вони не повинні прямо спонукати неповнолітніх купувати або брати напрокат продукт або послугу, користуючись їх недосвідченістю та довірливістю, прямо заохочувати їх до того, щоб переконати батьків або інших придбати рекламовані товари або послуги, використовувати довіру неповнолітніх до батьків, вчителів або	Audiovisual Media Services Directive (Article 9).

	інших осіб, або безпідставно показувати неповнолітніх у небезпечних ситуаціях. Держави-члени повинні заохочувати використання співрегулювання та сприяти впровадженню саморегулювання стосовно неналежних аудіовізуальних комерційних повідомлень, що супроводжують дитячі програми або включені до них, стосовно харчових продуктів та напоїв, що містять поживні речовини та речовини з поживним або фізіологічним ефектом, зокрема жири, трансжирні кислоти, сіль або соду та цукор, надмірне вживання яких у загальному раціоні не рекомендується.Такі кодекси повинні бути спрямовані на ефективне зниження впливу на дітей аудіовізуальних комерційних повідомлень про такі харчові продукти та напої. Вони повинні бути спрямовані на те, щоб аудіовізуальні комерційні повідомлення не наголошували на позитивних якостях поживних аспектів таких харчових продуктів та напоїв.	
2.1.6. Обмеження свободи вираження поглядів, пов'язані з захистом дітей	Законодавство щодо захисту неповнолітніх не застосовується у спосіб, який обмежує публічні дискусії з питань суспільного інтересу. Таке законодавство накладає обмеження на свободу вираження поглядів тільки у відповідь на нагальні суспільні потреби, що повинні визначатися якомога вужче, та передбачає співмірні санкції. При цьому, адекватними є часові та інші обмеження на контент, що може негативно вплинути на здоров'я неповнолітніх, а заборона на дитячу порнографію є абсолютною. Держава вживає необхідних законодавчих або інших заходів для запобігання всім формам сексуальної експлуатації та сексуального насильства стосовно дітей і для захисту дітей. Держава має вживати ефективні заходи для запобігання та припинення торгівлі дітьми, дитячої проституції і дитячої порнографії.	Audiovisual Media Services Directive (Article 6a); Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Article 4, 20); Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (Article 1).
	Держава вживає таких законодавчих та інших заходів, які можуть бути необхідними для визнання кримінальними злочинами, коли вони вчиняються умисно, наступних діянь: • виготовлення дитячої порнографії з метою її розповсюдження через комп'ютерну систему;	Convention on Cybercrime (Article 9).

	• пропонування або надання доступу до дитячої порнографії через комп'ютерну систему; • розповсюдження або передача дитячої порнографії через комп'ютерну систему; • придбання дитячої порнографії через комп'ютерну систему для себе або для іншої особи; • зберігання дитячої порнографії в комп'ютерній системі або на комп'ютерному носії інформації.	
2.1.7. Обмеження свободи вираження поглядів, пов'язані з підтриманням авторитету і безсторонності суду	Окрім випадків нападів, що є серйозно шкідливими та явно необґрунтованими, судді як представники однієї з основоположних інституцій держави можуть бути об'єктом персональної критики в межах, допустимих у демократичному суспільстві. Виконуючи свої офіційні обов'язки, вони підпадають під ширші межі допустимої критики, ніж пересічні громадяни.	ECtHR, Morice v. France (para. 131).
	Свобода вираження поглядів є однією з основоположних засад демократичного суспільства та необхідною умовою його розвитку й самореалізації кожної особи. Вона охоплює не лише ті висловлювання, що сприймаються позитивно або вважаються нейтральними, а й ті, які можуть ображати, шокувати чи тривожити — такі є вимоги плюралізму, толерантності й відкритості, без яких неможливе демократичне суспільство. Як передбачено статтею 10 Конвенції, свобода вираження може бути обмежена, але будь-яке таке обмеження повинно бути чітко визначене законом і переконливо обґрунтоване необхідністю у демократичному суспільстві. Судові органи, як і будь-які інші державні інституції, не є захищеними від критики та громадського контролю.	ECtHR, Skałka v. Poland (paras. 32, 34).
	Преса виконує ключову роль у демократичному суспільстві як один з основних механізмів поширення інформації та формування громадської думки. Хоча журналісти не повинні порушувати встановлені межі, зокрема щодо захисту репутації та прав інших осіб, на них покладено обов'язок поширювати – з дотриманням професійних стандартів та відповідальності – інформацію й ідеї з усіх питань, що становлять суспільний інтерес, включаючи функціонування судової влади.	ECtHR, De Haes and Gijsels v. Belgium (para. 37).

	Свобода вираження поглядів адвокатів тісно пов'язана з незалежністю юридичної професії, яка є вирішальною передумовою ефективного здійснення справедливого правосуддя. Адвокати зобов'язані завзято захищати інтереси своїх клієнтів, що іноді вимагає від них висловлення критики, подання заперечень або скарг на дії суду. Водночас така критика повинна залишатися в межах професійної відповідальності та не переходити у надмірні або необґрунтовані напади.	ECtHR, Morice v. France (paras. 135, 137).
2.2. Свобода медіа		
2.2.1. Свобода діяльності медіа, плюралізм та редакційна незалежність	Медіа не зобов'язані отримувати спеціальний дозвіл чи ліцензію для здійснення своєї діяльності онлайн чи ведення блогів (крім реєстрації підприємницької діяльності, якщо необхідно).	European Media Freedom Act (Article 4).
	Держава забезпечує доступ до різноманіття медіа в інтересах вільного і демократичного дискурсу, зокрема за допомогою механізмів законодавства з захисту економічної конкуренції.	European Media Freedom Act (Articles 3, 22).
	Незалежність редакційної політики медіа гарантується у законодавстві та на практиці. Медіа не стають об'єктом тиску щодо включення або видалення певної інформації або вимог дотримуватися певного напрямку редакційної політики.	European Media Freedom Act (Article 4).

2.2.2. Захист журналістських джерел та конфіденційність комунікацій	Держава забезпечує ефективний захист журналістських джерел і конфіденційних комунікацій, надаючи до них доступ лише у виняткових випадках, за попереднім дозволом судових чи інших незалежних органів, коли це виправдано переважним суспільним інтересом та є пропорційним. Щоб уникнути обходу принципу захисту журналістських джерел і конфіденційних комунікацій, гарантії повинні також поширюватися на осіб, які через свої регулярні приватні або професійні стосунки з провайдерами медіапослуг або членами їхніх редакцій можуть володіти інформацією, що може ідентифікувати журналістські джерела або конфіденційні комунікації - осіб, які перебувають у близьких стосунках, а також осіб, які професійно займаються або займалися підготовкою, виробництвом або поширенням програм чи публікацій у пресі, технічний персонал, включаючи експертів з кібербезпеки та ін. Забезпечення належного рівня захисту журналістських джерел і конфіденційних комунікацій вимагає, щоб заходи для отримання такої інформації були санкціоновані органом (наприклад, судом), який може незалежно і неупереджено оцінити, чи виправдані вони переважаючим суспільним інтересом. Заходи стеження підлягають регулярному перегляду таким органом для з'ясування того, чи продовжують виконуватися умови, що виправдовують застосування відповідного заходу. Право на ефективний судовий захист має включати своєчасне інформування, без шкоди для ефективності поточних розслідувань, про заходи стеження, вжиті без відома зацікавленої особи з метою ефективного здійснення цього права. Інтрузивне програмне забезпечення для стеження повинно застосовуватися лише тоді, коли це виправдано переважаючим суспільним інтересом, передбачено законом, було санкціоновано ex ante або, у виняткових і невідкладних випадках, згодом підтверджено судовим органом або іншим незалежним і неупередженим органом, що приймає рішення, стосується розслідування вчинення відповідною особою тяжких злочинів, за які передбачено покарання у вигляді позбавлення волі, і за умови, що жоден інший, менш суворий, захід не був би адекватним і достатнім для одержання потрібної інформації.	European Media Freedom Act (Article 4);

	Зважаючи на важливість захисту журналістських джерел інформації для свободи преси у демократичному суспільстві, обмеження конфіденційності журналістських джерел інформації вимагають найретельнішого розгляду. Втручання, яке потенційно призводить до розголошення джерела інформації, не може вважатися «необхідним», якщо тільки воно не виправдано першочерговою вимогою в інтересах суспільства. Для встановлення існування «першочергової вимоги» не може бути достатнім лише доведення стороною, яка прагне розголошення джерела, що без розголошення інформації вона не зможе здійснювати законне право або запобігти загрозі вчинення правопорушення, на якій ґрунтується її клопотання: міркування, які мають враховуватися судом, схиляють баланс конкуруючих інтересів на користь інтересів демократичного суспільства у забезпеченні свободи преси. У зв'язку з цим право журналістів не розголошувати їхні джерела інформації не може розглядатися як звичайний привілей, який надається або якого позбавляють залежно від законності чи незаконності їхніх джерел інформації, а є невід'ємною частиною права на інформацію, до якого слід ставитися максимально обачно.	ЄСПЛ, Седлецька проти України (пара. 62)
2.2.3. Захист від перешкоджання журналістській діяльності у цифровому середовищі	Держави-учасниці повинні забезпечити комплексну законодавчу базу, яка надасть змогу журналістам та іншим учасникам медіа брати участь у громадських обговореннях ефективно та без остраху. Законодавство, яке криміналізує насильство щодо журналістів, необхідно підсилювати системою, яка забезпечить його застосування, і механізмами компенсації постраждалим (та їхнім сім'ям), які мають бути ефективними на практиці. Необхідно сформулювати чітке положення про форми тимчасового захисту у вигляді судової заборони й превентивних заходів для тих, хто стикається із загрозою насильства. Державам рекомендується розробити протоколи й навчальні програми для всіх органів державної влади, які є відповідальні за виконання державних зобов'язань щодо захисту журналістів та інших учасників медіа. Держави-учасниці зобов'язані вживати ефективних заходів, що необхідні для притягнення до відповідальності всіх осіб, які скоїли злочини проти журналістів та інших медіаучасників.	Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors

2.2.4. Незалежний та ефективний регуляторний орган у сфері медіа	Держави повинні забезпечити, щоб національні регуляторні органи: ● здійснювали свої повноваження неупереджено та прозоро, в дусі медіаплюралізму, захисту споживачів, доступності, відсутності дискримінації, сприяння добросовісній конкуренції тощо; ● не запитували і не отримували від будь-якого іншого органу вказівки щодо виконання завдань, покладених на них згідно з положеннями національного права; ● мали чітко визначені у законі компетенції та повноваження, а також способи забезпечення їх підзвітності; ● отримували адекватні фінансові, технічні та людські ресурси для ефективного виконання покладених на них функцій. Держави повинні визначити у національному праві умови та процедури призначення та звільнення керівників національних регуляторних органів будь-якого рівня або членів колегіального органу, що виконують цю функцію, включно з тривалістю їх мандату. Такі процедури повинні бути прозорими, недискримінаційними та гарантувати необхідний рівень незалежності.	Audiovisual Media Services Directive (Article 30); European Media Freedom Act (Article 7).
2.3. Свобода вираження поглядів та онлайн-платформи		
2.3.1. Зобов'язання держави щодо захисту прав користувачів онлайн-платформ	Законодавство, що застосовується до онлайн-платформ, незалежно від сфери їх діяльності, повинне ефективно захищати права людини та застосовуватися недискримінаційно, хоча і з врахуванням різних розмірів та функцій таких платформ. Держава має забезпечити аби компанії, що перебувають під її юрисдикцією: ● враховували при розробці своїх внутрішніх політик, що стосуються здійснення свободи вираження поглядів, міжнародні стандарти у цій сфері; ● забезпечували прозорість у сфері модерації контенту, зокрема публікували власні правила модерації контенту та щорічно публікували звіти про прозорість; ● надавали користувачам пояснення причин обмеження їх права на свободу вираження поглядів на платформі; ● розкривали основні параметри функціонування рекомендаційних систем та алгоритмів на платформах;	Digital Services Act; Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (paras. 2.2.1, 2.2.3, 2.2.4, 2.3.3, 2.5.1); Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business (paras. 5, 15); Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy Framework'; Audiovisual Media Service Directive (Article 28b).

	• створювали ефективні засоби захисту та системи вирішення спорів, що будуть доступними, справедливими та прозорими, зокрема механізми notice-and-action. Держава вживає належних заходів для розбудови інфраструктури захисту права користувачів на свободу вираження поглядів, зокрема шляхом сертифікації позасудових органів вирішення спорів, затвердження довірених партнерів та гарантування права дослідників до доступ до інформації для моніторингу дотримання онлайн-платформами прав користувачів.	
2.3.2. Статус та вимоги до онлайн-платформ щодо дотримання принципів свободи вираження поглядів	Онлайн-платформам має бути гарантований імунітет від відповідальності за поширення на їх платформах протиправного контенту, окрім випадків, коли вони отримують належні відомості про наявність протиправного контенту та не вживають належних заходів для його обмеження достатньо швидко. Будь-яке втручання в діяльність онлайн-платформ, що може призвести до обмеження свободи вираження користувачів, має відповідати принципам законності, легітимності та необхідності у демократичному суспільстві та має здійснюватися судом або іншим незалежним адміністративним органом. Законодавство має встановлювати вимоги щодо інформації, що має міститися у запиті на обмеження доступу до контенту, яка буде достатньою для його ідентифікації. Держава не може покладати на онлайн-платформи зобов'язання щодо загального моніторингу власних мереж на предмет пошуку протиправного контенту чи діяльності.	Digital Services Act (Articles 6, 8, 9); Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (paras. 1.1.1, 1.3.1, 1.3.5, 1.3.7).
2.3.3. Незалежний та ефективний регуляторний орган у сфері онлайн-платформ	Будь-які компетентні органи, залучені до регулювання онлайн-платформ, мають бути незалежними від зовнішнього впливу, а також забезпечені належними технічними, фінансовими та людськими ресурсами для нагляду над усіма суб'єктами, що перебувають під їх юрисдикцією.	Digital Services Act (Articles 49-50); Audiovisual Media Service Directive (Article 30).

2.4. Свобода вираження поглядів в умовах воєнного стану		
2.4.1. Обмеження свободи вираження поглядів під час воєнного стану	Відступ держави від зобов'язань у сфері свободи вираження поглядів допускається виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов'язанням згідно з міжнародним правом. Обмеження права на отримання та поширення інформації мають бути законними, пропорційними та необхідними для досягнення легітимних цілей. Будь-які запроваджені обмеження мають бути переглянуті та скасовані після закінчення дії правового режиму воєнного стану.	European Convention on Human Rights (Article 15).
2.4.2. Правові підстави та порядок блокування інтернет-ресурсів під час війни	Правила блокування інтернет-ресурсів під час воєнного стану мають бути чітко встановлені законодавством, бути необхідними та пропорційними та спрямовуватися на досягнення легітимного інтересу захисту національної безпеки. Органи, що здійснюють таке блокування, мають належно оприлюднювати рішення про обмеження доступу до ресурсу та зазначати причини його ухвалення, з подальшим переглядом після закінчення правового режиму воєнного стану.	European Convention on Human Rights (Articles 10, 15); International Covenant on Civil and Political Rights (Articles 4, 19).
3. ПРАВО НА ПОВАГУ ДО ПРИВАТНОГО ЖИТТЯ В ЦИФРОВОМУ СЕРЕДОВИЩІ		
3.1. Захист персональних даних		
3.1.1. Законодавчі гарантії захисту персональних даних	Законодавство закріплює право особи на захист її персональних даних.	Treaty on the Functioning of the European Union (Article 16); Charter of Fundamental Rights of the European Union (Article 8); Конвенція про захист прав людини і основоположних свобод (стаття 8).

	Національне законодавство встановлює достатні гарантії захисту персональних даних у відповідності з вимогами Ради Європи та Європейського Союзу. Такі гарантії включають необхідну та пропорційну обробку персональних даних відповідно до основоположних принципів та на легітимних основах (зокрема, за згоди суб'єкта), заборону обробки чутливих даних (за винятком випадків, передбачених законом), забезпечення суб'єкта даних рядом прав, а також належний нагляд за дотриманням законодавства.	General Data Protection Regulation (Recitals 10, 32, 53); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Chapter II).
	Відповідні гарантії суб'єктів даних повинні забезпечуватися якщо обробка даних відбувається за допомогою ШІ-систем або сама інформація була отримана шляхом використання інтрузивних технологій.	UNESCO Recommendations on Ethics of AI (para. 33).
	Закон закріплює наявність контролера та процесора. Контролером є фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, а також інші фізичні або юридичні особи, для яких цілі та засоби обробки визначені законом. Процесором є фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який здійснює обробку персональних даних від імені контролера.	General Data Protection Regulation (Articles 4(7), 4(8)).
	Закон повинен чітко визначати обов'язки контролера. Контролер впроваджує відповідні технічні та організаційні заходи для демонстрації правомірності обробки персональних даних (відповідні заходи підлягають регулярному перегляду). Такі заходи можуть також включати впровадження належних політик захисту даних контролером.	General Data Protection Regulation (Article 24).
	Закон закріплює концепцію спільних контролерів, за якої цілі та засоби обробки персональних даних визначаються спільно двома або більше контролерами. Спільні контролери зобов'язані визначити та розподілити їх обов'язки стосовно дотримання вимог обробки персональних даних у домовленості, яка повинна бути оприлюднена суб'єкту даних. Домовленість може передбачати, який з контролерів буде відповідальним за комунікацію з суб'єктом даних. Суб'єкт даних може здійснювати свої права щодо кожного з контролерів незалежно від умов домовленості. Обмін однаковими даними між контролерами, використання спільних баз даних та інфраструктури без спільних засобів та мети обробки даних не становить спільного контролерства.	General Data Protection Regulation (Article 26); Guidelines 07/2020 on the concepts of controller and processor in the GDPR (paras. 70-71).

	Закон передбачає захист персональних даних за проєктуванням та замовчуванням. Контролер зобов'язаний при визначенні засобів обробки персональних даних та протягом такої обробки вжити належних технічних та організаційних заходів, які забезпечують належне та ефективне дотримання принципів, підстав обробки персональних даних та впровадження захисних гарантій в процес обробки персональних даних. Кожен контролер зобов'язаний вжити належних технічних та організаційних заходів для забезпечення того, щоб за замовчуванням оброблялися виключно ті персональні дані, які необхідні для досягнення визначеної легітимної мети обробки. Такий обов'язок стосується обсягу персональних даних, які збираються, обсягу обробки персональних даних, строку зберігання та доступності персональних даних.	General Data Protection Regulation (Article 25).
	Закон повинен чітко визначати обов'язки процесора, який обробляє дані від імені контролера. Обробка даних процесором здійснюється на підставі контракту або іншого правового акту, який повинен адресувати: ● предмет обробки даних (наприклад, записи з камер відеостеження осіб, які заходять та виходять з об'єкту); ● тривалість обробки даних; ● характер обробки (наприклад, «архівування» або «запис»); ● мету обробки (наприклад, виявлення незаконного проникнення); ● вид персональних даних; ● категорії суб'єктів даних (наприклад, «відвідувачі», «працівники»); ● обов'язки та права контролера. Крім того, в контракті зазначається, зокрема, що процесор: ● обробляє персональні дані виключно за наявності письмового доручення контролера, яке включає, зокрема, питання щодо передачі персональних даних іншим державам або міжнародним організаціям; ● вживає заходів для забезпечення захисту персональних даних; ● з урахуванням характеру обробки, сприяє дотриманню контролером обов'язку відповідати на запити суб'єктів персональних даних щодо реалізації їх прав;	General Data Protection Regulation (Article 28(1), 28(3)); Guidelines 07/2020 on the concepts of controller and processor in the GDPR (para. 114).

	• на вимогу контролера видаляє або повертає всі персональні дані контролеру після закінчення надання послуг з обробки персональних даних тощо.	
	Процесор не має залучати іншого процесора без попереднього загального чи спеціального письмового дозволу контролера. У випадку надання дозволу процесор зобов'язаний повідомити контролера про намір такого залучення або заміни з метою надання контролеру можливості заперечити проти цього.	General Data Protection Regulation (Article 28(2)).
	Якщо процесор залучив іншого процесора для здійснення певних процесів з обробки даних від імені контролера, залучений процесор має ті самі обов'язки, які передбачені контрактом або правовим актом, на підставі якого здійснюється обробка від імені контролера. Якщо залучений процесор не виконує покладених на нього обов'язків з захисту персональних даних, відповідальність за порушення ним зобов'язань перед контролером несе процесор, який здійснив залучення.	General Data Protection Regulation (Article 28(4)).
	Кожен контролер (або представник контролера) зобов'язаний здійснювати реєстрацію операцій з обробки персональних даних, за яку контролер несе відповідальність. Відповідні записи повинні містити інформацію про: • найменування або ім'я, контактні дані контролера, та, у разі наявності, – спільного контролера, представника контролера та відповідальної особи з питань захисту персональних даних; • мету обробки; • опис категорій суб'єктів персональних даних та категорій персональних даних; • категорії одержувачів, яким персональні дані були або можуть розкриватись; • передачу персональних даних іншим державам або міжнародним організаціям; • строк для видалення різних категорій персональних даних у разі, якщо це можливо; • загальний опис технічних та організаційних заходів з безпеки.	General Data Protection Regulation (Article 30).
3.1.2. Дотримання загальних принципів	Закон встановлює принципи правомірної обробки персональних даних: законність, добросовісність та прозорість, обмеження мети, мінімізація даних, точність персональних даних, обмеження строків зберігання, цілісність, конфіденційність, підзвітність.	General Data Protection Regulation (Article 5);

та підстав обробки персональних даних		Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 5).
	Закон встановлює чіткий перелік підстав обробки персональних даних: ● згода суб'єкта даних на обробку його персональних даних; ● укладення та виконання правочину, стороною якого є суб'єкт даних; ● необхідність виконання юридичного обов'язку контролера; ● захист життєво важливих інтересів суб'єкта даних або іншої фізичної особи; ● необхідність виконання завдань в суспільних інтересах або повноважень, покладених на контролера законом; ● необхідність для цілей досягнення легітимного інтересу контролера або третьої особи, крім випадків, коли такі інтереси не переважають інтереси або основоположні права та свободи суб'єкта персональних даних. Окремі національні закони/положення можуть уточнювати інші законні підстави.	General Data Protection Regulation (Article 6).
	Закон повинен встановити належний механізм надання та відкликання згоди суб'єкта даних на обробку його даних. Згода становить вільне, чітке, інформоване та однозначне волевиявлення суб'єкта даних, виражене у формі заяви та/або чіткої стверджувальної дії, яким він дозволяє обробку своїх персональних даних. Якщо згода суб'єкта даних надається у письмовій формі, запит на таку згоду повинен бути поданий у зрозумілій та легкодоступній формі з використанням чіткої та простої мови. Згода на обробку даних може бути відкликана суб'єктом даних у будь-який момент. У випадку обробки даних неповнолітньої особи, згода батьків/опікунів є обов'язковою.	General Data Protection Regulation (Articles 4(11), 7, 8); Guidelines 05/2020 on consent under Regulation 2016/679 (Chapter 3).
	Закон забороняє обробку персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в професійних спілках, а також генетичних та біометричних даних, даних, що стосуються здоров'я, статевого життя або сексуальної орієнтації. Закон передбачає чіткий перелік випадків, за яких така обробка є правомірною.	General Data Protection Regulation (Article 9).

	Чутливі персональні дані можуть піддаватися автоматичній обробці виключно за наявності належних гарантій у національному законодавстві.	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 6).
	Законодавство передбачає підстави для обробки персональних даних, пов'язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості. При цьому закон передбачає належні гарантії для прав та свобод суб'єкта даних.	General Data Protection Regulation (Recital 19, Article 10); Law Enforcement Directive (Articles 2, 8).
3.1.3. Дотримання прав суб'єктів персональних даних	Законодавче закріплення права на інформацію, права на доступ до персональних даних, права на виправлення даних, права на забуття (див. п. 3.1.4.), права на заперечення та обмеження обробки даних, права на мобільність персональних даних, права на захист від автоматизованого прийняття рішення, а також відшкодування шкоди та відновлення порушених прав.	General Data Protection Regulation (Articles 13, 15-18, 20-21).
	У випадку зібрання даних від суб'єкта даних, контролер зобов'язаний надати суб'єкту даних таку інформацію: ● особу та контактні дані контролера (де доречно, його представника); ● (де доречно) контактні дані офіцера захисту даних; ● правову основу та мету обробки даних; ● уточнення легітимних інтересів контролера, якщо обробка відбувається для їх захисту; ● одержувачів або категорії одержувачів персональних даних, якщо такі є; ● (де доречно) повідомлення про те, що контролер має намір передати персональні дані третій країні або міжнародній організації.	General Data Protection Regulation (Article 13(1)).
	У випадку зібрання даних від суб'єкта, який не є суб'єктом даних, контролер зобов'язаний надати суб'єкту даних таку інформацію: ● особу та контактні дані контролера (де доречно, його представника); ● (де доречно) контактні дані офіцера захисту даних; ● правову основу та мету обробки даних; ● категорії персональних даних, що обробляються; ● одержувачів або категорії одержувачів персональних даних, якщо такі є; ● де доречно, повідомлення про те, що контролер має намір передати персональні дані третій країні або міжнародній організації.	General Data Protection Regulation (Article 14(1)).

	При реалізації «права на доступ» контролер повинен надати повну, правильну та актуальну інформацію, що максимально відповідає стану обробки даних на момент отримання запиту. Така інформація включає підтвердження/спростування факту обробки даних, а також: ● мету обробки; ● категорію відповідних персональних даних; ● одержувачів або категорій одержувачів, яким персональні дані були або будуть розкриті, (зокрема, одержувачів в третіх країнах або міжнародні організації); ● якщо можливо, передбачуваний період зберігання персональних даних, або, якщо це неможливо, критерії для визначення такого періоду; ● наявність права вимагати від контролера виправлення або видалення персональних даних або обмеження чи заперечення проти обробки даних; ● право подання скарги до наглядового органу; ● будь-яку доступну інформація щодо джерела збору даних (якщо персональні дані не збираються суб'єктом даних); ● наявність автоматизованого прийняття рішень, у тому числі профайлингу, а також змістовну інформацію про значення та наслідки такої обробки для суб'єкта даних.	General Data Protection Regulation (Article 15(1)); Guidelines 01/2022 on data subject rights - Right of access (para. 34).
	Будь-яка інформація від контролера до суб'єкта даних повинна бути надана у чіткій, прозорій, зрозумілій та легкодоступній формі, з використанням зрозумілої та ясної мови. Інформація надається у письмовій або іншій формі, включаючи електронну форму.	General Data Protection Regulation (Article 12).
	Закон закріплює право суб'єкта даних на виправлення контролером неточних персональних даних щодо нього без надмірної затримки.	General Data Protection Regulation (Article 16).
	Особа реалізує право на обмеження обробки даних, якщо: ● точність персональних даних оскаржується суб'єктом даних протягом періоду, що дозволяє контролеру перевірити достовірність персональних даних; ● обробка є незаконною, а суб'єкт даних виступає проти видалення персональних даних і натомість вимагає обмеження їх використання;	General Data Protection Regulation (Article 18(1)).

	• суб'єкт даних потребує даних для встановлення, здійснення або захисту правових вимог; • суб'єкт даних заперечив проти обробки до перевірки законності того, чи переважають підстави контролера над підставами суб'єкта даних.	
	Закон закріплює право на мобільність персональних даних, за якого особа має право вимагати від контролера надання копії будь-яких персональних даних такого суб'єкта у структурованому та машинозчитувальному форматі, за умови що: • обробка здійснюється на підставі згоди суб'єкта даних; • обробка здійснюється на підставі договору; • обробка здійснюється за допомогою автоматизованих засобів.	General Data Protection Regulation (Article 20).
	Особа може заперечити обробку її персональних даних у будь-який момент – у такому випадку контролер припиняє обробляти дані, якщо не буде надано обґрунтованих законних підстав для обробки, які переважатимуть інтереси, права та свободи суб'єкта даних або встановлюватимуть або захищатимуть правові вимоги. Особа може заперечити проти обробки даних для науково чи історично дослідницьких або статистичних цілей, за винятком випадку, коли така обробка є необхідною для виконання завдань, яке виконується з міркувань суспільного інтересу.	General Data Protection Regulation (Article 21(1),(6)).
	Закон закріплює право особи на захист від автоматизованого прийняття рішення, включаючи профайлинг, яке має юридичні наслідки або інший значний вплив для суб'єкта даних.	General Data Protection Regulation (Article 22).
	Суб'єкт даних має право на засоби правового захисту, які включають право оскарження дій наглядового органу, а також право на судовий захист щодо діяльності наглядового органу, контролера або процесора.	General Data Protection Regulation (Articles 77-79); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 10).
	Підстави та перелік обмежень щодо прав мають бути чіткими і обґрунтованими, а також законодавчо встановленими.	General Data Protection Regulation (Article 23).
	Положення щодо обмеження прав повинні адресувати: • категорії персональних даних ;	General Data Protection Regulation (Article 23);

	• обсяг обмежень (наприклад, які права буде обмежено і на який період часу); • гарантії проти зловживань та неправомірного доступу або передачі даних (включає запровадження технічних або організаційних заходів); • уточнення контролера (аби суб'єкт знав, до кого звертатися у випадку обмеження); • періоди зберігання даних; • ризики правам та свободам суб'єкта даних (для оцінки пропорційності та впливу обмежень); • право на повідомлення про обмеження.	Guidelines 10/2020 on restrictions under Article 23 GDPR (Chapter 4).
	Закон закріплює право бути забутим та передбачає чіткий перелік підстав для реалізації суб'єктом даних такого права. Серед таких випадків: • персональні дані більше не є необхідними для цілей, для яких вони були зібрані; • суб'єкт даних відкликав згоду на обробку даних, а інша підстава для обробки даних відсутня; • суб'єкт даних заперечує проти обробки даних, а переважаючі законні підстави для обробки відсутні; • персональні дані були оброблені неправомірно; • персональні дані мають бути видалені для дотримання юридичних зобов'язань у законодавстві Європейського Союзу або держав-членів, до яких підлягає контролер; • персональні дані були зібрані у зв'язку з пропозицією послуг інформаційного суспільства.	General Data Protection Regulation (Article 17); Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) (Chapter 1).
	Закон повинен встановити механізм реалізації права бути забутим, який може включати: • видалення, зміну, анонімізацію відповідної інформації, або обмеження її доступності у мережі; • технічні заходи щодо повідомлення контролера про вимогу суб'єкта видалити його дані; • можливість оскарження рішення при відмові реалізувати право бути забутим.	General Data Protection Regulation (Article 17); ECtHR, M.L. and W.W. v. Germany (paras. 59-60).

	Закон повинен передбачити чіткий перелік легітимних винятків, коли право бути забутим не може бути реалізоване, а обробка даних є необхідною, зокрема: • для реалізації права на свободу вираження поглядів та інформації; • для дотримання юридичного обов'язку контролера; • з міркувань суспільного інтересу у сфері громадського здоров'я; • для цілей архівування в суспільних інтересах, наукових чи історичних дослідницьких цілей, або • для статистичних цілей; • для встановлення, здійснення або захисту правових вимог.	General Data Protection Regulation (Article 17); Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) (Chapter 2); ECtHR, Hurbain v Belgium (para. 251).
3.1.4. Внутрішні інструменти дотримання стандартів захисту персональних даних	У разі, якщо обробка даних передбачає вищі ризики для суб'єктів, держава має зобов'язати контролера даних здійснювати оцінку впливу на захист даних. Така оцінка є обов'язковою у випадках: • систематичної та широкої автоматизованої обробки, включно з профілюванням, для оцінки особистих аспектів фізичних осіб, і прийняття рішень, які спричиняють юридичні наслідки або суттєво впливають на особу; • масштабної обробки спеціальних категорій даних або персональних даних, що стосуються кримінальних засуджень і правопорушень; • систематичного широкомасштабного моніторингу публічних місць. Оцінка впливу на захист даних має здійснюватися у випадках, якщо види обробки є в переліку EDPS. Така оцінка має містити: • системний опис операцій з обробки даних і їх цілей, включаючи законний інтерес контролера; • оцінка необхідності та пропорційності операцій обробки відносно цілей; • оцінка ризиків для прав і свобод суб'єктів; • заходи, передбачені для усунення ризиків. Оцінка впливу може включати комунікацію з суб'єктами даних, без розкриття комерційної таємниці чи іншої конфіденційної інформації. Якщо контролер не впевнений, що заходи зможуть адекватно зменшити ризики для прав, він має проконсультуватися з наглядовим органом.	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+) (Article 10(2)); Explanatory Report to Convention 108+ (paras. 88-89); General Data Protection Regulation (Articles 35-36); Decision of the EDPS of 16 July 2019 on DPIA Lists issued under Articles 39(4) and (5) of GDPR (Annex 1).
	Держава має закріпити обов'язок призначати відповідальну особу з захисту даних у випадках, коли:	General Data Protection Regulation (Articles 37-39).

	• обробка здійснюється державним органом або установою (за винятком судів); • основна діяльність контролера або оператора передбачає операції з обробки, які через характер, обсяг та/або цілі потребують регулярного та систематичного моніторингу суб'єктів; • основна діяльність контролера або оператора полягає в масштабній обробці спеціальних категорій даних, що стосуються кримінальних засуджень і правопорушень. Декілька суб'єктів можуть призначити спільну особу, відповідальну за захист даних. Така особа має мати відповідні компетенції, а також мати необхідні для виконання своїх повноважень ресурси та функціональну і адміністративну незалежність. Її контактні дані мають бути публічно доступними. Мінімальні функції особи, відповідальної за захист даних, передбачають обов'язок: • інформувати і консультувати контролера або оператора та працівників, які виконують обробку щодо їхніх зобов'язань із захисту даних; • контролювати дотримання законодавства щодо захисту даних і політики контролера або оператора, включаючи розподіл обов'язків, навчання персоналу та пов'язані з ними аудити; • надавати консультації щодо оцінки впливу на захист даних і контролювати її виконання; • співпрацювати з наглядовим органом; • бути контактною особою для наглядового органу і проводити консультації у разі необхідності.	
	Державні органи мають сприяти розробці та підписанню індустрією кодексів поведінки, зокрема щодо: • чесної та прозорої обробки; • законних інтересів контролерів у конкретних контекстах; • збору персональних даних; • псевдонімізації персональних даних; • інформації, яка надається громадськості та суб'єктам даних; • здійснення прав суб'єктів даних; • інформації, яка надається дітям, захисту дітей, згоди на обробку даних дітей; • заходів для забезпечення безпеки обробки;	General Data Protection Regulation (Articles 40-41).

	• сповіщення контролюючих органів про порушення та повідомлення суб'єктів про порушення; • передача персональних даних третім країнам або міжнародним організаціям; • позасудове провадження і процедури вирішення спорів між контролерами і суб'єктами даних. Кодекси поведінки мають передбачати механізми, моніторинг виконання яких може здійснити наглядовий орган. Кодекси поведінки реєструються наглядовим органом, який робить їх публічно доступними в єдиному реєстрі. Моніторинг дотримання кодексів поведінки здійснює орган, який: • продемонстрував незалежність та експертність щодо предмета кодексу; • встановив процедури, які дозволяють оцінювати право контролерів і операторів застосовувати кодекс; • встановив процедури та механізми для розгляду скарг щодо порушень кодексу, зробив їх прозорими для суб'єктів даних і громадськості; • довів наглядовому органу відсутність конфлікту інтересів. Такий орган отримує акредитацію у наглядового органу та може, за наявності порушень, видаляти контролерів та операторів з підписантів кодексів.	
	Держава має заохочувати розробку сертифікаційних механізмів, печаток та маркування захисту даних для демонстрації дотримання законодавчих вимог. Процес сертифікації має бути добровільним і прозорим, а сертифікація дійсною не довше 3 років з можливістю поновлення. Сертифікація має здійснюватися сертифікаційним органом, чиї повноваження засвідчені наглядовим органом або національним акредитаційним органом. Вимоги до сертифікаційного органу включають: • незалежність і досвід щодо предмета сертифікації; • зобов'язання дотримуватися вимог щодо сертифікації; • наявність процедур видачі, перегляду і відкликання сертифікатів, печаток і маркування; • наявність процедур та механізмів розгляду скарг щодо порушень сертифікації, їх прозорість для суб'єктів даних та громадськості; • відсутність конфлікту інтересів.	General Data Protection Regulation (Articles 42-43).
	У випадку транскордонної передачі даних держава має забезпечити належний рівень захисту даних через: належні гарантії на рівні інших держав	Modernised Convention for the Protection of Individuals with Regard to the

3.1.5. Вільний обіг даних	або обов'язкові корпоративні правила компаній, які оброблятимуть дані. Також передача можлива за наявності прямої згоди особи чи легітимного інтересу (і якщо заходи є необхідними і пропорційними).	Processing of Personal Data (Convention 108+), (Article 14); Explanatory Report to Convention 108+ (paras. 110-114).
	Держава має забезпечити право на мобільність персональних даних і їх вільну передачу від контролера до контролера за наявності згоди і автоматизації таких процесів. Транскордонна передача персональних даних може здійснюватися, якщо суб'єкт, що оброблятиме дані забезпечує належний рівень їх захисту; держава або компанія (на рівні корпоративних правил або кодексів поведінки) мають впровадити належні гарантії і запобіжники від зловживань. Корпоративні правила мають передбачати права суб'єктів даних, можливість оскаржувати рішення щодо обробки, а також механізми співпраці з наглядовим органом.	General Data Protection Regulation (Articlei 20, 45-47); Standard Contractual Clauses Decision International Transfer SCCs Decision.
	Обробка даних трафіка не має розкривати змісту комунікацій і має здійснюватися не довше, ніж це необхідно для виконання легітимної мети. Дані щодо місцезнаходження користувачів можуть оброблятися лише за умови анонімізації або за наявності згоди. Спам чи адресні рекламні повідомлення без згоди користувача мають бути заборонені.	E-Privacy Directive (Articles 6, 9, 13).
	Користувачі мають право на мобільність даних і доступ до даних генерованих продуктами інтернету речей, включно з тим, як дані структуровані та що з ними можна робити. Володільці даних мають уможливлювати доступ третіх сторін до даних на запит користувачів (із паралельним застосуванням вимог законодавства про захист персональних даних). Доступ до даних може надаватися на оплатній основі із розумною компенсацією. Дані можуть надаватися у випадку невідкладних обставин, а також на запит публічних органів (у визначених випадках).	Data Act (Articles 3, 5, 9, 15-17).
	Дані, володільцями яких є публічні органи та які належать до комерційної таємниці чи статистичних конфіденційних даних, захищені правом інтелектуальної власності або є персональними даними можуть повторно використовуватися на підставі окремих договорів на визначений строк (не довше 12 місяців) і за певних умов (наприклад, анонімізація персональних даних чи конфіденційної інформації). Держава має встановити окремі вимоги	Data Governance Act (Articles 5, 10-11, 16-17).

	до сервісів посередників щодо отримання доступу до даних, зокрема процедура повідомлення наглядового органу про діяльність. Держава має допомагати суб'єктам персональних даних реалізувати право на альтруїзм даних (добровільне поширення даних на підставі згоди для їх використання в суспільно важливих цілях).	
	Документи, видані суб'єктами в публічному секторі або такі, що стосуються питань публічного сектору (як-от авіаперевезення чи надання публічних послуг приватними суб'єктами), а також дані досліджень мають бути публічно доступними (за винятком персональних даних) безоплатно. Такі документи мають бути у форматі відкритих даних за проєктуванням і за замовчуванням. Динамічні дані (дані транзакцій) мають бути доступними для повторного використання.	Open Data Directive (Articles 3, 5, 6).
	Вимоги локалізації даних (за винятком питань публічної безпеки) мають бути заборонені. Держави мають заохочувати підписання кодексів поведінки у сфері перенесення даних (англ. «data porting»), включно зі створенням можливостей для швидкої зміни провайдерів послуг електронних комунікацій.	Free Flow of Non-Personal Data Regulation (Article 4).
	Держава має врегулювати діяльність посередників та постачальників послуг онлайн-пошуковиків, за допомогою яких бізнес та корпоративний сектор можуть пропонувати товари і послуги. Це, зокрема, передбачає встановлення вимог прозорості до посередників і постачальників, а також який режим доступу бізнес-користувачів до персональних даних пропонують такі суб'єкти.	Platform-to-Business Regulation (Articles 3, 4, 5, 7, 9).
3.1.6. Заборонені практики у сфері захисту даних	Держава має заборонити обробку особливих (чутливих) категорій персональних даних про расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, членство в профспілках, генетичних і біометричних даних, даних щодо стану здоров'я, статевого життя чи сексуальної орієнтації. У законодавстві повинні бути чітко визначені винятки із заборони: ● явна згода суб'єкта даних; ● необхідність обробки для здійснення прав та виконання обов'язків контролера у трудовій сфері; ● необхідність обробки для захисту життєво важливих інтересів суб'єкта даних чи іншої особи;	General Data Protection Regulation (Recitals 51-56, Article 9); Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), (Article 6); ECtHR, Catt v the United Kingdom (2019), (para. 112); ECtHR, S. and Marper v the United Kingdom [GC] (2008), (para. 76);

	• обробка даних неприбутковими організаціями (у політичних, релігійних, світоглядних, профспілкових цілях) із гарантіями захисту та лише щодо їхніх членів чи осіб, які підтримують регулярні контакти; • обробка даних, що були явно оприлюднені суб'єктом даних; • необхідність обробки для подання, обґрунтування чи захисту правових вимог, та в судових цілях; • необхідність обробки у цілях суспільного інтересу; • необхідність обробки у сфері охорони здоров'я і соціального забезпечення; • необхідність обробки для охорони громадського здоров'я; • необхідність обробки у цілях суспільного інтересу, наукового чи історичного дослідження або статистики.	CJEU, C-136/17, GC and Others v Commission nationale de l'informatique et des libertés (CNIL) (paras. 44-45, 80).
	Держава має заборонити прийняття рішень, які мають правові наслідки для особи чи іншим чином істотно впливають на неї, виключно на підставі автоматизованої обробки персональних даних, у тому числі профайлінгу. Детальніше ці стандарти описані у пункті 4.4.2 Методології.	General Data Protection Regulation, Recital 71 (Article 22); Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), (Article 6); Recommendation CM/Rec(2021)8 on the protection of individuals with regard to automatic processing of personal data in the context of profiling (paras. 3.13-14); CJEU, C-634/21, SCHUFA Holding (Scoring) (para. 75).
	Держава має заборонити скрейпінг біометричних даних. Заборони підлягають системи ШІ, які створюють чи розширюють бази даних розпізнавання облич шляхом нецільового скрейпінгу зображень облич з інтернету чи записів камер відеоспостереження. Наприклад, систему *Clearview AI* визнали винною у такому скрейпінгу.	Artificial Intelligence Act (Recital 43, Article 5.1(e)); General Data Protection Regulation (Article 9(1)); Dutch DPA's decision (Clearview AI) (paras. 8, 29, 73, 96, 205).
	Держава має встановити заборону на системи категоризації осіб на основі біометричних даних, що розкривають расову приналежність, політичні погляди, членство в профспілках, релігійні чи філософські переконання,	Artificial Intelligence Act (Recital 30, Article 5.1(g)); Law Enforcement Directive (Article 10).

	статеве життя чи сексуальну орієнтацію особи. У законодавстві мають бути чітко визначені винятки з цієї заборони для: ● маркування чи фільтрації законно отриманих наборів біометричних даних (зокрема зображень); ● категоризації біометричних даних у правоохоронній сфері.	
	Держава має заборонити використання систем дистанційної біометричної ідентифікації в режимі реального часу в публічних місцях. У законодавстві мають бути чітко й деталізовано визначені винятки з цієї заборони щодо правоохоронних органів, детальніше описані у пункті 4.4.3 Методології.	Artificial Intelligence Act (Recitals 32-33, 38-41, Article 5.1(h)-5.5); Law Enforcement Directive (Article 10).
	Держава має заборонити системи ШІ, які використовують дані осіб про вік, інвалідність, конкретну соціальну чи економічну ситуацію з метою суттєвого спотворення їхньої поведінки, що спричиняє або обґрунтовано може спричинити значну шкоду.	Artificial Intelligence Ac (Recital 29, Article 5.1(b)).
	Держава має заборонити системи ШІ, що на основі особливих даних визначають емоції осіб на робочих місцях і в навчальних закладах, за винятком випадків, пов'язаних із медичними чи безпековими причинами.	Artificial Intelligence Act (Recital 44, Article 5.1(f)).
	Держава має заборонити системи ШІ, що оцінюють чи прогнозують ризики вчинення особою правопорушення виключно на основі її профайлінгу або оцінки її особистісних ознак. Водночас ця заборона не поширюється на системи ШІ, які допомагають людській оцінці причетності особи до кримінальної діяльності, що ґрунтується на об'єктивних фактах, які можна перевірити. Детальніше про це йдеться у пункті 4.5.2 Методології.	Artificial Intelligence Act (Recital 42, Article 5.1(d)).
	Держава має встановити заборону на профайлінг, що призводить до дискримінації осіб на основі особливих (чутливих) персональних даних.	Law Enforcement Directive (Article 11(3).
	На онлайн-платформах не повинна демонструватись реклама на основі профайлінгу із використанням особливих (чутливих) персональних даних.	Digital Services Act (Article 26(3).
	Держава має на законодавчому рівні заборонити обробку персональних даних неповнолітніх осіб у комерційних цілях, зокрема у цілях прямого маркетингу, профайлінгу та поведінково таргетованої реклами (англ. «behaviourally targeted advertising»).	AVMSD (Article 6a(2)); Digital Services Act (Article 28(2)); Recommendation CM/Rec(2018)7 (Guidelines to respect, protect and fulfil the rights of the child in the digital environment) (paras. 37, 57).
3.2. Приватність та безпека у цифровому середовищі		

3.2.1. Захист честі, гідності та ділової репутації	Закони про дифамацію є чіткими і відповідають міжнародним стандартам. Вони не перешкоджають публічним дебатам або критиці державних органів і не накладають надмірних штрафів або непропорційних збитків або судових витрат. Дифамація не є криміналізованою. Серйозні санкції можуть застосовуватися лише у випадках, коли висловлювання призводять до тяжких наслідків, на кшталт насильства, повалення конституційного ладу, дискримінації тощо.	General Comment 34 to Article 19 of the ICCPR; ECtHR, Lingens v. Austria (para. 46), ECtHR, Castells v. Spain (para. 42); ECtHR, Radio France and Others v. France (para. 40); Audiovisual Media Services Directive (Article 28);
	Без обмеження інших положень, згідно з цивільним, адміністративним або кримінальним правом, будь-яка фізична або юридична особа, чиїм законним інтересам, зокрема, честі і репутації було завдано шкоди внаслідок подання неправдивих фактів, повинна мати право на відповідь або рівноцінні засоби захисту своїх прав. Держави повинні забезпечити, щоб фактичному застосуванню права на відповідь або рівноцінних засобів захисту прав не перешкоджало встановлення необґрунтованих строків або умов. Відповідь повинна бути трансльована протягом розумного часу після обґрунтування вимоги на таку відповідь та в строк і спосіб, що відповідає трансляції програми, якої стосується вимога. Заява про здійснення права на відповідь або вжиття еквівалентних засобів захисту може бути відхилена, якщо відповідь є необґрунтованою, порушує закон, призведе до відповідальності медіа або порушить стандарти громадської порядності.	
3.2.2. Право на зображення	Національне законодавство закріплює право особи на зображення та встановлює гарантії щодо захисту такого права.	ECtHR, Von Hannover v. Germany (no. 2) (para. 96).
	Закон повинен наділяти особу правом контролювати використання її зображень, включаючи право на заборону публікації таких зображень.	ECtHR, Von Hannover v. Germany (no. 2) (para. 103).
	При публікації зображень важливо враховувати ступінь популярності особи та її публічну роль, а також публічний інтерес громадськості у відповідних публікаціях (включаючи випадки, коли опубліковано зображення непублічної особи, яка залучена у ситуацію з публічними фігурами).	ECtHR, Von Hannover v. Germany (para. 60); ECtHR, Flinkkilä and Others v. Finland (para. 85).

	Законодавство повинно встановлювати гарантії щодо захисту зображень неповнолітніх осіб (наприклад, встановлювати механізм попередньої згоди батьків/опікунів на публікацію).	ECtHR, Reklos and Davourlis v. Greece (para. 41); ECtHR, Bogomolova v. Russia (para. 56).
	У контексті поширення зображень національні правила повинні належним чином балансувати приватність та свободу вираження поглядів з урахуванням таких факторів: ● внесок публікації в обговорення суспільного інтересу; ● ступінь відомості особи та предмет публікації; ● попередня поведінка особи, зображення якої було опубліковано; ● зміст, форма і наслідки публікації; ● обставини, за яких були зняті відповідні фотографії.	ECtHR, Von Hannover v. Germany (no. 2) (paras. 108-113); ECtHR, Hájovský v. Slovakia (paras. 33-49).
	Законодавство повинно закріплювати право особи на людську гідність та індивідуальну автономію щодо діяльності систем ШІ.	Framework Convention on Artificial Intelligence, and Human Rights, Democracy, and the Rule of Law (Article 7); UNESCO Recommendations on Ethics of AI, para. 32.
	Законодавство має встановлювати вимоги щодо маркування генерованого контенту, в тому числі якщо він містить фото, відео чи голос особи.	Artificial Intelligence Act (Article 50(4)).
3.2.3. Гарантування анонімності та безпеки онлайн	Персональні дані особи можуть оброблятися у випадках, передбачених в законодавстві або коли особа дала на це згоду (наприклад, погоджуючись на умови використання Інтернет-сервісу, включаючи, зокрема, файли «cookies» але маючи можливість відкликати таку згоду).	Explanatory Memorandum to Recommendation CM/Rec(2014)6 (paras. 69-71).
	Принципи захисту даних повинні застосовуватися до псевдонімізованої інформації, якщо з її допомогою отримувач може ідентифікувати особу, у протилежному випадку така інформація не вважатиметься персональними даними і не підлягатиме захисту.	Regulation 2018/1725 (para. 16); SRB v EDPS (paras. 100-103).
	Держава повинна захищати право на конфіденційність усіх приватних комунікацій онлайн та поважати бажання Інтернет-користувачів не	Council of Europe Recommendation on internet intermediaries (para. 1.4.3);

	розкривати свою особу для захисту проти онлайн стеження та захисту свободи вираження поглядів.	Declaration on freedom of communication on the Internet (Principle 7); Standard Verlagsgesellschaft mbH v. Austria (no. 3), (para. 80).
	Держава має забезпечити посилений захист конфіденційних даних, зокрема обробка даних, що включає конфіденційні чи біометричні дані (наприклад, розпізнавання обличчя), не повинна активуватися за замовчуванням.	Recommendation on the protection of human rights with regard to social networking services (para. 15).
	Дані про місцезнаходження (окрім даних трафіку) можуть оброблятися тільки коли стають анонімними, або зі згоди користувача.	EU Directive on privacy and electronic communications (Article 9(1)).
	Будь-яке державне втручання в персональні дані користувачів, яке може обмежити їхнє право на приватність (включаючи накладання обмежень на анонімність, отримання доступу до зашифрованих даних), повинне бути передбачене законом, переслідувати легітимну мету та бути необхідним в демократичному суспільстві.	Council of Europe Recommendation on internet intermediaries (para. 1.4.1); OECD Guidelines for Cryptography Policy (Guideline 6); UNHRC Report on encryption and anonymity (para. 31).
	Користувач повинен мати безкоштовну і просту у реалізації можливість запобігати небажаним комунікаціям (телефонним дзвінкам, електронним листам тощо), пов'язаним з його діями в Інтернеті (ідентифікація номера, автоматичні дзвінки, маркетингові комунікації тощо).	EU Directive on privacy and electronic communications (Articles 8, 11, 13).
	Як під час визначення методів обробки даних, так і під час самої обробки контролер має вживати необхідні технічні та організаційні заходи, такі як псевдонімізація та шифрування, для безпеки та захисту прав суб'єкта даних.	General Data Protection Regulation (Article 32).
	Задля уникнення незаконного доступу третіх осіб до інформації, законодавство має захищати використання засобів шифрування, включаючи ті, що створені для захисту анонімності (наприклад, не забороняти їх і не вимагати їхню реєстрацію перед використанням), і впроваджувати заборони на такі засоби тільки у виключних обставинах: коли вони законні, необхідні, пропорційні та переслідують легітимну мету.	Special Rapporteur Encryption and Anonymity follow-up report (paras. 47-49); Recommendation on the protection of human rights with regard to social networking services (para. 15).
	Посередники (платформи, провайдери електронних комунікацій тощо) не можуть розкривати персональну інформацію користувачів третім особам, за винятком випадків, коли таке розкриття здійснюється за вимогою суду чи іншого адміністративного органу (зокрема, слідчого), чиї рішення підлягають судовому перегляду, який визначив, що таке розкриття відповідає	Appendix to Recommendation CM/Rec(2018)2 (para. 2.4.1); ECtHR, Delfi As v Estonia (para. 148).

	законодавству та стандартам, є необхідним у демократичному суспільстві та пропорційним легітимній меті.	
	Розкриття анонімної інформації органам безпеки та розвідки провайдерами електронних комунікацій можливе тільки за таких умов: цільовий доступ до великих обсягів даних (заборона загальної і невибіркової передачі інформації), необхідність авторизації (окрім надзвичайних ситуацій) перед отриманням доступу, повідомлення про здійснення такого доступу користувачу.	Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (para. 52); Watson and Others (paras. 110, 112, 121).
	Створення «backdoors» чи інших засобів для послаблення чи обходу заходів безпеки або використання їхніх існуючих недоліків (наприклад, надання ключів шифрування третім особам) має бути заборонено національним законодавством держави і не використовуватися державою.	Resolution on mass surveillance (para. 19.1); Special Rapporteur Encryption and Anonymity follow-up report (para. 49); ECtHR, Podchasov v. Russia (para. 79).
	Держава має на законодавчому рівні заборонити перехоплення чи стеження за приватними комунікаціями користувача. Держава може не забороняти такі дії на законодавчому рівні у випадку, коли вони є легальними у зв'язку з провадженням бізнесу, або користувач надав згоду на це, чи такі дії відповідають процедурним стандартам та необхідні для цілей захисту національної безпеки або стосуються боротьби зі злочинами.	EU Directive on privacy and electronic communications (Article 5); Convention on Cybercrime (Article 3).
	Держава має уповноважити відповідні органи на збирання даних, які можуть бути необхідними у зв'язку з розслідуванням серйозних злочинів, якщо це необхідно для уникнення реальної небезпеки чи припинення конкретного кримінального правопорушення.	Convention on Cybercrime (Article 21); Recommendation No. R (87) 15 (Principle 2.1).
	Державні заходи стеження повинні бути цільовими, чітко визначеними, з ефективним зовнішнім наглядом, здатним забезпечити прозорість та відповідальність за державне спостереження за комунікаціями, їхнє перехоплення та збір персональних даних. Обставини застосування цих заходів мають бути чітко визначеними, про що детальніше йдеться у пунктах 3.3.2 та 3.3.3 Методології.	UNGA Resolution 68/167 (para. 4(d)); Council of Europe Recommendation on internet intermediaries (para. 1.4.4); ECtHR, Podchasov v. Russia (para. 64).
	Необхідні заходи безпеки мають вживатися для захисту персональних даних, які зберігаються в файлах даних для автоматизованої обробки, від випадкового або неавторизованого знищення чи втрати, а також від несанкціонованого доступу, зміни або поширення.	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 7).

	Суб'єкт даних повинен мати можливість: ● встановити наявність файлу даних, придатного для автоматизованої обробки, його основні цілі, характер, місцезнаходження чи роботи контролера; ● отримувати в розумні строки та у зрозумілій формі підтвердження, чи зберігаються його персональні дані в файлах даних для автоматизованої обробки; ● вимагати виправлення або знищення даних, якщо вони оброблялися всупереч законодавству; ● використовувати засоби правового захисту в разі невиконання прохання про підтвердження або про надання, виправлення або знищення персональних даних.	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 8).
	У державі повинні існувати органи, відповідальні за управління ризиками у сфері кібербезпеки та органи нагляду за дотриманням принципів щодо безпеки та анонімності онлайн.	NIS 2 Directive (Articles 20-21); Recommendation No. R (87) 15 (Principle 1.1); Additional Protocol to the Convention 108+ (Article 1).
	Держава повинна запровадити санкції та ефективні засоби захисту в разі порушення законодавства у сфері гарантування безпеки онлайн.	NIS 2 Directive (Article 36); Convention 108 (Article 10); Council of Europe Recommendation on internet intermediaries (para. 1.5).
3.2.4. Протидія кібербулінгу, порнопомсті, гендерно зумовленому насильству	Держава має заборонити онлайн-шахрайство, дитячу порнографію і будь-які форми онлайн-насилля. Держава має запобігати таким активностям, впроваджувати технічні та організаційні заходи для цього.	Convention on Cybercrime (Articles 7, 8, 9).
	Онлайн-цькування (кібербулінг)	
	Сервіси, що можуть використовуватися дітьми, повинні мати належні гарантії захисту приватності, безпеки та захищеності. Оцінка впливу системних ризиків на права людини має враховувати потенційні негативні впливи на фізичне і психологічне здоров'я і благополуччя дітей.	Digital Services Act, (Articles 28, 34).
	Провайдери платформ спільного доступу до відео мають вживати заходів, щоб захищати дітей від програм, користувацьких відео і реклами, які можуть нашкодити їх фізичному і психологічному розвитку.	Audiovisual Media Services Directive (Article 28b(1)(a)).

	Держава має законодавчо заборонити вчинення спільно з іншими особами за допомогою інтернету публічно доступних погрозливих або образливих дій, спрямованих на особу, якщо така поведінка може спричинити їй серйозну психологічну шкоду. Держава має вимагати видалення такої категорії контенту або ж обмеження доступу до неї.	Directive on combating violence against women and domestic violence (Articles 7(1)(b), 23).
	Держави повинні заохочувати бізнес та інших стейкхолдерів розробляти та впроваджувати політики, спрямовані на боротьбу з кібербулінгом, переслідуваннями та розпалюванням ненависті та насильства онлайн. Такі політики повинні описувати неприйнятну поведінку, механізми повідомлення та заходи підтримки дітей, які постраждали від таких дій.	Recommendation CM/Rec(2018)7 on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (paras. 50-51, 59); European Parliament Resolution of 3 May 2018 on media pluralism and media freedom in the EU (para. 26).
	Держава має впроваджувати заходи медіа і цифрової грамотності щодо новітніх викликів, породжених технологіями, повідомляти зацікавлених стейкхолдерів про ризики та можливі шляхи їх вирішення. Держава має розробляти стратегії запобігання кібербулінгу щодо дітей, розробляти універсальні законодавчі визначення таких концепцій.	Strategy for the Rights of the Child (2022-2027), (page 14); Council Resolution on the EU Youth Strategy 2019-2027 (ANNEX 3);
	Порнопомста (поширення інтимних зображень без згоди)	
	Держава має впровадити концепцію права на забуття, яка в тому числі дозволить постраждалим від порнопомсти вчасно і належним чином видаляти таку інформацію з мережі.	General Data Protection Regulation (Article 17).
	Дуже великі онлайн-платформи мають надати постраждалим від поширення без згоди інтимних зображень механізми для оскарження та швидкого видалення такого контенту, а також проводити оцінку ризиків щодо гендерно зумовленого насильства (що включає і порнопомсту).	Digital Services Act (Recital 87, Article 34).
	Провайдери генеративних систем штучного інтелекту (ШІ) мають забезпечити дотримання принципу прозорості. Генерований контент має належно маркуватися для запобігання діпфейкам, в тому числі порнофейкам.	Artificial Intelligence Act (Articles 3(44)(b)(I), 50(2)).

	Держава має заборонити оприлюднення за допомогою інформаційно-комунікаційних технологій зображень, відео чи подібного матеріалу, що зображує відверті дії сексуального характеру або інтимні частини особи, без згоди цієї особи, якщо така поведінка може завдати їй серйозної шкоди, а також погрози вчинити такі дії з метою примусити особу вчинити або відмовитися від вчинення певних дій. Держава має заборонити виробництво, маніпулювання або зміну і подальше оприлюднення в онлайн просторі зображень, відео чи подібного матеріалу, що створює враження, ніби особа бере участь у відверто сексуальних діях, без згоди цієї особи, якщо це може завдати їй серйозної шкоди, а також погрози вчинити такі дії з метою примусити особу вчинити або відмовитися від вчинення певних дій.	Directive on combating violence against women and domestic violence (Article 5(1)(a)(b)(c)).
	Держави мають вживати всіх необхідних заходів, щоб попереджати будь-які форми насильства, в тому числі і психологічного (яке є одним з наслідків порнопомсти). Порнопомста є одним з порушень в онлайн просторі, який часто є частиною переслідувань особи або домагань, і має бути кримінально караною тією ж мірою, що і аналогічні дії в реальному житті.	Istanbul Convention (Articles 12(2), 33, 34, 40); GREVIO General Recommendation No. 1 on the digital dimension of violence against women (page 18).
	Держава має заборонити участь дітей у порнографічних активностях, поширення дитячої порнографії, домагання і сексуальну експлуатацію дітей. Держава має створити ефективні та безпечні механізми для повідомлення про такі порушення.	Lanzarote Convention (Articles 12, 20-21).
	Держава має заборонити будь-які форми дитячої порнографії, а також належним чином захищати приватність постраждалих від таких дій.	Directive on combating sexual abuse and sexual exploitation of children (Article 5).
	Держави мають створити регуляторну рамку, в межах якої існують інструменти повідомлення про сексуалізований контент за участі дітей, поширений на платформах, та ефективні засоби правового захисту в таких обставинах.	European Parliament Resolution on child sexual abuse online (paras. 12-13, 19).
	Гендерно зумовлене насилля онлайн	
	Платформи мають щонайменше раз на рік (та у випадках критичних збоїв у функціоналі, які впливають на права людини) здійснювати пошук і оцінку системних ризиків (які включають гендерно зумовлене насилля) серед: • дизайну систем рекомендацій і будь-яких інших схожих алгоритмічних систем;	Digital Services Act (Article 34).

	• системи модерації контенту; • умов користування (політик платформ) та їх застосування на практиці; • системи відбору та подання реклами; • практик, пов'язаних з даними.	
	Заборона неправомірної поведінки за ознакою гендеру, зокрема заборона психологічного насильства, домагань та переслідувань застосовна в онлайн-просторі тією ж мірою, що і офлайн. Держави мають встановлювати додаткові зобов'язання для платформ щодо запобігання такій діяльності як публічно, так і в приватних комунікаціях, впроваджуючи організаційні та технічні заходи.	Istanbul Convention, (Articles 12(2), 33, 34, 40); GREVIO General Recommendation No. 1 on the digital dimension of violence against women (pages 17-23).
	Держава має законодавчо заборонити такі дії: • постійне спостереження за особою в інтернеті без згоди цієї особи або законного дозволу на це для відстеження або моніторингу за пересуваннями та діяльністю цієї особи, якщо така поведінка може завдати їй серйозної шкоди; • неодноразову чи постійну участь у загрозливих онлайн-діях, спрямованих на особу, принаймні якщо така поведінка передбачає погрози вчинення кримінальних правопорушень та може викликати у цієї особи серйозні побоювання за власну безпеку або безпеку утриманців; • непогоджене надсилання зображення, відео чи іншого подібного матеріалу із зображенням геніталій особі, якщо така поведінка може спричинити їй серйозну психологічну шкоду; • оприлюднення в онлайн просторі матеріалів, що містять персональні дані особи, без її згоди з метою спонукати інших осіб до заподіяння їй фізичної чи серйозної психологічної шкоди; • підбурювання до насильства чи ненависті, спрямованих проти групи осіб або члена такої групи, визначених за ознакою гендеру. Держава також має вимагати видалення таких категорій контенту або обмеження доступу до них.	Directive on combating violence against women and domestic violence (Articles 5(1)(b)(c), 6, 7, 8, 23).
	Публічні заклики до ворожнечі чи насильства є забороненими (на будь-якій захищеній підставі).	Audiovisual Media Services Directive (Article 6).

	При розробці політик, законів, інших регуляторних інструментів у сфері протидії гендерно зумовленого насилля, держави мають залучати громадянське суспільство та жінок до розробки таких актів. Таке законодавство, зокрема, має охоплювати теми онлайн погроз, переслідувань, цькувань та домагань, торгівлі людьми, а також закликів до насилля і мови ворожнечі. Остання категорія має охоплювати розпалювання ворожнечі на підставі статі та гендеру.	Recommendation CM/Rec(2019)1 on Preventing and Combating Sexism (section I.A); Parliamentary Assembly Resolution 2144 on ending cyberdiscrimination and online hate (paras. 2, 7.2.2); European Parliament Resolution with recommendations to the Commission on combating gender-based violence: cyber violence (paras. 15-18, 24-26, 31).
3.3. Стеження		
3.3.1. Встановлення та дотримання гарантій прав людини під час застосування заходів стеження	Заходи стеження повинні здійснюватися відповідно до доступного, чіткого, конкретного та передбачуваного закону. Закон повинен чітко та точно встановлювати: ● вичерпний перелік підстав, за яких уповноважені органи можуть вдаватися до заходів стеження; ● компетентні державні органи, які мають повноваження здійснювати заходи стеження, сферу та обсяг їх дискреції, спосіб її реалізації виходячи із легітимної цілі відповідного заходу; ● природу порушень, щодо яких можуть застосовуватися заходи стеження; ● категорії осіб щодо яких можуть застосовуватися заходи стеження; ● обмеження щодо застосування заходів стеження; ● процедури щодо аналізу, використання та зберігання інформації, отриманої за допомогою заходів стеження; ● запобіжні заходи щодо передачі отриманих даних іншим особам та заходи щодо безпеки передачі даних; ● підстави для знищення або видалення інформації, отриманої за результатами стеження та ін.	ECtHR, Roman Zakharov v Russia (paras. 229-231); General Data Protection Regulation (Article 6).
	Закон повинен передбачити пропорційний період тривалості заходів стеження, який супроводжується гарантіями для суб'єкта даних (наприклад, завершення заходів стеження по досягненню переслідуваної мети або вичерпання строку дії авторизації).	ECtHR, Roman Zakharov v Russia (paras. 250-251).

	Закон повинен передбачити чіткий та пропорційний період зберігання інформації, отриманої внаслідок заходів стеження, а також механізм видалення даних за умови, що вони більше не є необхідними. Варто передбачити перелік суб'єктів, які мають доступ до даних, а також заходи безпеки щодо збереження їх конфіденційності. У випадку зберігання чутливих даних, закон повинен містити додаткові заходи безпеки щодо запобігання несанкціонованого доступу або витоку таких даних (наприклад, збереження даних в окремих базах або їх шифрування).	ECtHR, Ekimdzhiev and Others v Bulgaria (paras. 329-330); ECtHR, Gaughran v the United Kingdom (para. 94); Guidelines 3/2019 on processing of personal data through video devices (paras. 88-89); Law Enforcement Directive (Article 5).
	При зверненні до заходів стеження для цілей запобігання кримінальним правопорушенням, закон повинен встановлювати вичерпний перелік злочинів (які досягли достатнього рівня тяжкості), при підозрі або вчиненні яких органи можуть вдаватися до заходів стеження. Закон також повинен розрізняти між категоріями осіб, над якими здійснюється стеження, серед яких: підозрюваний, обвинувачений, жертва та інші сторони.	Law Enforcement Directive (Article 6); ECtHR, Roman Zakharov v Russia (paras. 244-245); ECtHR, Ekimdzhiev and Others v Bulgaria (para. 302).
	Заходи стеження над журналістами, представниками медіа або видавцями можуть здійснюватися у виключних випадках, передбачених законом, які виправдані необхідністю досягнення мети щодо розслідування злочинів та переважаючим публічним інтересом. Такі заходи можуть здійснюватися лише якщо мета не може бути досягнута іншими способами, та повинні супроводжуватися відповідними гарантіями суб'єктів даних.	European Media Freedom Act (Article 4(4)).
	Закон повинен передбачити механізм авторизації заходів стеження, який може здійснюватися судом або незалежним органом. Вимога на авторизацію повинна: ● посилатися на обставини, які дають підстави підозрювати, що відповідний злочин готується чи вчиняється або був скоєний; ● перелічити вже вчинені розслідувальні дії та їх результати; ● пояснити, чому необхідну інформацію неможливо отримати в інший спосіб; ● пояснити, чому необхідна запланована тривалість заходів стеження. Авторизація повинна бути належним чином обґрунтована та надана лише якщо стеження є законним, необхідним та виправданим (не містить альтернативних або менш інтрузивних заходів).	ECtHR, Roman Zakharov v Russia (para. 262); ECtHR, Ekimdzhiev and Others v Bulgaria (para. 309).

	Закон повинен встановлювати належний механізм нагляду перед, під час та після здійснення заходів стеження: ● суд, який авторизував стеження, повинен бути уповноважений на моніторинг імплементації заходів, а також їх судовий перегляд; ● наглядовий орган повинен бути інституційно незалежним та неупередженим (тобто незалежним від виконавчої гілки влади), а також наділений функціями щодо захисту прав суб'єктів даних; ● повинно гарантуватися публічне періодичне звітування відповідних органів про застосування заходів стеження.	ECtHR, Roman Zakharov v Russia (paras. 233, 283); ECtHR, Ekimdzhiev and Others v Bulgaria (para. 334); ECtHR, Szabo and Vissy v Hungary (para. 77).
	Закон повинен передбачити ефективні механізми правового захисту, які включають: ● повідомлення особи про здійснення заходів стеження, де доречно, перед початком таких заходів, та обов'язково після їх завершення; ● можливість особи вимагати від органів влади інформацію про зібрані дані та мати доступ до такої інформації; ● можливість оскарження правомірності заходів стеження до відповідних органів; ● можливість наглядового органу видати розпорядження щодо відновлення порушених прав за вимогою суб'єкта даних – наприклад, знищити дані, отримані внаслідок стеження.	Law Enforcement Directive (Article 14); ECtHR, Roman Zakharov v Russia (para. 291); ECtHR, Ekimdzhiev and Others v Bulgaria (para. 344); Guidelines 3/2019 on processing of personal data through video devices (paras. 92, 100, 105).
3.3.2. Обмеження масового стеження	Положення про систему масового стеження чітко передбачені законодавством, мають загальні гарантії аналогічні до тих, що застосовуються до звичайних заходів стеження (див. пункт 3.3.1).	ECtHR, Roman Zakharov v Russia (para. 262).
	Системи відеостеження в публічних місцях можуть встановлюватися виключно для досягнення легітимної мети та захисту легітимних інтересів, які повинні бути чітко окреслені. Закон повинен містити належно обгрунтовані підстави та цілі за яких здійснюється невибіркове стеження.	Guidelines 3/2019 on processing of personal data through video devices (paras. 15-17, 44); ECtHR, Klass v Germany (para. 41).
	Системи стеження повинні бути встановлені виключно уповноваженими органами, після отримання авторизації (судового дозволу) та піддаватися нагляду та моніторингу з боку незалежного органу.	ECtHR, Big Brother Watch and Others v the United Kingdom (paras. 348-349).

	Системи відеостеження повинні бути обладнаними спеціальними попередженнями про здійснення відеостеження. Суб'єкту, який піддається стеженню, повинна бути надана інформація про: • особу та контактні дані контролера; • мету обробки та (де доречно) індикатор, що обробка здійснюється системою розпізнавання облич; • право оскарження заходів до контролюючого органу та контактні дані такого органу; • право суб'єкта вимагати доступ до персональних даних, їх виправлення чи видалення та право на обмеження обробки персональних даних.	Guidelines 3/2019 on processing of personal data through video devices (paras. 112, 117); Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (para. 86).
	Системи розпізнавання облич не мають вдаватися до розпізнавання емоцій (за винятком медичних чи безпекових потреб).	Artificial Intelligence Act (Article 5(1)(f)).
	Забороняється використовувати системи ШІ, які створюють або розширюють бази даних розпізнавання облич за допомогою нецільового скрепінгу зображень облич з інтернету або записів камер відеостеження.	Artificial Intelligence Act (Article 5(1)(e)).
	Обробка чутливих даних для правоохоронних цілей може здійснюватися виключно якщо це передбачено законом, для захисту життєво важливих інтересів та якщо обробці підлягають дані, які явно оприлюднені суб'єктом даних. При обробці біометричних даних необхідно забезпечити додаткові гарантії для суб'єктів даних, які включають обов'язкове видалення первинних даних (зображення обличчя, мовні сигнали, хода тощо).	Law Enforcement Directive (Article 10); Guidelines 3/2019 on processing of personal data through video devices (para. 90).
	Перехоплення комунікацій може здійснювати винятково за наявності обґрунтованої підозри у вчиненні правопорушення, лише за наявності судового дозволу та обмежується вмістом комунікацій, які можуть становити розумний інтерес для слідства в контексті конкретної справи.	ECtHR, Weber and Saravia v Germany (para. 125); ECtHR, Big Brother Watch and Others v the United Kingdom (para. 348).
	Використання систем біометричної ідентифікації «в режимі реального часу» для правоохоронних цілей дозволяється виключно у випадку, коли вони використовуються таргетовано для пошуку потерпілих від злочину чи викрадених осіб, для попередження реальної загрози чи розслідування злочину.	Artificial Intelligence Act (Article 5(1)(h)).
3.3.3. Обмеження застосування	Держава має на законодавчому рівні забезпечити захист конфіденційності електронних комунікацій через публічно доступні електронні сервіси.	E-Privacy Directive (Article 5(1));

шпигунського програмного забезпечення	Прослуховування, запис, зберігання чи перехоплення приватних комунікацій має бути забороненим за винятком випадків, коли це є правомірним. Приховане стеження може здійснюватися лише для попередження та розслідування злочинної діяльності, в тому числі у сферах національної безпеки та оборони. Воно має бути цільовим і обґрунтованим (як-от обґрунтована підозра у вчиненні правопорушення).	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), (Article 11); Explanatory Report to Convention 108+ (paras. 91-98).
	Заборонено неправомірно (умисно і без дозволу) отримувати доступ до пристроїв, перехоплювати дані без належної авторизації (зокрема, в цілях національної безпеки чи попередження злочинів), а також виготовляти чи використовувати пристрої для здійснення такої неправомірної діяльності (зокрема, і поширення шкідливого програмного забезпечення, шахрайства за допомогою комп'ютерних систем та використання технологій стеження). Авторизація таких заходів має здійснюватися уповноваженим органом, наприклад, судом.	Convention on Cybercrime (Articles 2, 6, 15); T-CY Guidance Note #12 Aspects of ransomware covered by the Budapest Convention; T-CY Guidance Note #7 New forms of Malware.
	Держава має обов'язок захищати викривачів та забезпечувати їхню конфіденційність, за винятком випадків, коли викривачі самостійно вирішують публічно розкрити свою особу. Викривачі мають бути захищені від переслідувань. Держава не має права переслідувати викривачів, а також має забезпечити їм право на належний судовий захист та інші ефективні засоби правового захисту.	Whistleblower Directive (Articles 16, 21).
	Держава має врегулювати на законодавчому рівні засоби кібер-стеження – об'єкти подвійного використання, що уможливлюють моніторинг, збір і аналіз даних з електронних комунікаційних систем. Для виготовлення, обігу і використання таких засобів мають бути встановлені спеціальні правила, зокрема, авторизація розробників і розповсюджувачів, та дозвільна система у сфері експорту/імпорту таких технологій.	Dual-Use Regulation (Articles 2, 5, 26).

	Використання програмного забезпечення для моніторингу, шантажу, маніпуляцій чи дискредитації опозиції, правозахисників, медіа чи активістів, маніпуляцій виборами чи підриву довіри до демократичних інституцій є неправомірним. Незаконна торгівля такими технологіями порушує права людини. Використання програмного забезпечення Pegasus порушує права людини. Pegasus та схоже програмне забезпечення мають бути забороненими, адже вони порушують саму сутність права на приватність, будучи непропорційним втручанням за будь-яких обставин. Оскільки Pegasus через свою невибірковість записує інформацію про третіх осіб, його використання не може бути виправданим. Крім того, він збирає надмірну кількість чутливої інформації, наприклад, про сексуальну орієнтацію, здоров'я та політичні погляди.	Report of the investigation in relation to the use of Pegasus and equivalent spyware (paras. 446, 462, 470-472); EU Parliament recommendation following the investigation in relation to the use of Pegasus and equivalent surveillance spyware (paras. 3, 8, 9, 97); EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (pages 11-12); EDPS Preliminary Remarks on Modern Spyware (page 9); PACE Report, Pegasus and similar spyware and secret state surveillance (para. 72); PACE Resolution on Pegasus and similar spyware and secret State surveillance (paras. 7-8, 12-13).
	До випадків використання шпигунського і шкідливого програмного забезпечення застосовні загальні стандарти у сфері стеження (описані у пункті 3.3.1 Методології). Перехоплення, обшук, вивчення та використання інформації з приватних комунікацій є втручанням у права всіх сторін комунікації. Стандарт доведення, що особа є постраждалою у справах, що стосуються перехоплення комунікацій, є низьким. Національне законодавство має передбачити випадки, коли можуть застосовувати засоби перехоплення комунікацій, а також гарантії від зловживань. Таке втручання може мати форму, зокрема, і отримання інформації про IP-адреси.	ECtHR, Wieder and Guarnieri v the United Kingdom (paras. 93-95, 99, 104); ECtHR, Zakharov v Russia (para. 229); ECtHR, Benedik v Slovenia (para. 132).

	Загальне і невибіркове збереження даних про трафік та місцезнаходження заборонено навіть для боротьби зі злочинністю чи забезпечення національної безпеки. При загальному зборі метаданих важливо, щоб не було отримано доступ до змісту комунікацій. Збір конкретних даних дозволений за наявності серйозної загрози національній безпеці під належним наглядом. Докази, отримані за допомогою шпигунського програмного забезпечення, не повинні порушувати права на справедливий судовий розгляд, докази мають належним чином оформлюватися і зберігатися. Держави мають повідомляти інші країни, якщо перехоплення комунікацій зачіпає їх громадян.	CJEU, Joined Cases C-511/18 and C512/18 (La Quadrature du Net and Others) (paras. 172, 177, 187-189, 216-228); CJEU C-623/17, Privacy International (paras. 68-71); CJEU Case C-670/22 ('EncroChat' case) (paras 20-25, 30-33, 40-45); CJEU C-293/12 and C-594/12, Digital Rights (paras. 39-40).
3.4. Наглядовий орган та заходи захисту права на повагу до приватного життя		
3.4.1. Незалежність та ефективність наглядового органу у сфері захисту персональних даних	Створення або призначення незалежного державного органу, що буде відповідальним за моніторинг виконання законодавства про захист даних, з метою захисту основоположних прав людини, пов'язаних з обробкою їх персональних даних. Гарантії незалежності включають: ● прозору процедуру призначення членів; ● визначений строк повноважень; ● наперед визначені вимоги до членів, в тому числі до їх компетенції; ● правила щодо конфлікту інтересів.	General Data Protection Regulation (Articles 51-54).
	При дизайнуванні наглядового органу державі потрібно враховувати: ● незалежність органу не означає відсутність моніторингу чи контролю за його діяльністю; ● доброчесність членів та відсутність у них іншої несумісної з роботою в органі зайнятості; ● наглядовий орган мусить мати власний персонал, відібраний або ним особисто, або іншим незалежним органом.	General Data Protection Regulation (Recitals 118, 121).
	Держава має визначити такі гарантії незалежності: ● склад органу; ● тривалість виконання та умови припинення їхніх функцій; ● можливість брати участь у відповідних засіданнях без надмірних обмежень;	Explanatory Report for Convention 108+ (Article 15).

	• можливість консультуватися з технічними та іншими експертами або проводити зовнішні консультації; • наявність достатніх ресурсів у органу; • можливість наймати власний персонал; • прийняття рішень без зовнішнього втручання, прямого чи опосередкованого. Незалежна діяльність автоматично передбачає заборону на запит чи отримання вказівок (окрім консультацій експертів). Окремою гарантією для підтримки є право суб'єктів оскаржити рішення органу в судовому порядку.	
	Держава має забезпечити такі гарантії: • наглядовий орган має бути відокремленим від загальної системи органів держави (такі органи не входять до жодної вертикальної системи підпорядкування, що виключає контроль з боку інших органів); • контроль з боку парламенту (інших політичних органів) має бути необхідним та ефективним, безпосередньо не втручаючись у роботу органу.	Case C-518/07, Judgment of the CJEU (Grand Chamber) of 9 March 2010.
	Державний орган має бути забезпечений усіма необхідними ресурсами для виконання своїх повноважень – як в частині достатніх повноважень, так і в частині таких ресурсів: • належне ресурсне забезпечення (людське, фінансове, технічне); • належна кваліфікація членів органу; • достатній обсяг повноважень для реалізації функцій (в тому числі можливість накладення санкцій); • можливість доводити порушення до відома судових органів та брати участь у судових процесах.	General Data Protection Regulation (Articles 55-59).
	Наглядовий орган обов'язково повинен мати такі загальні повноваження: • проведення розслідувань; • виправні повноваження та накладення санкцій; • дозвільні та консультативні повноваження; • право накладати тимчасове або остаточне обмеження на обробку даних, включаючи заборону. Кожен захід має бути доречним, необхідним і пропорційним. Варто уникати надмірних витрат і незручностей для осіб, що звернулися до наглядового	General Data Protection Regulation Recitals (129).

	органу. Ухвалення юридично обов'язкового рішення означає, що воно може бути предметом судового перегляду.	
	Мінімальні повноваження наглядового органу мають включати: • розслідування; • втручання; • винесення рішень з приводу порушень, що може включати адміністративні санкції (що мають бути ефективними, пропорційними та стримуючими); • можливість подання суб'єктами заяв та/або скарг; • можливість визначення пріоритетності таких скарг/заяв; • право надавати висновки щодо будь-яких законодавчих або адміністративних заходів, що передбачають обробку персональних даних; • процесуальну правоздатність органу.	Explanatory Report for Convention 108+ (Article 15).
	Якщо держава-член вирішує створити єдиний національний наглядовий орган, він обов'язково повинен мати всі повноваження, передбачені міжнародними стандартами. Наглядові органи можуть знищувати незаконно оброблені дані з власної ініціативи.	Case C-33/22, Judgment of the CJEU (Grand Chamber) of 16 January 2024 (ст. 18-21); Case C-46/23, Judgment of the CJEU (Fifth Chamber) of 14 March 2024.
	Втручання здійснюються лише у випадках та в спосіб, передбачені законом, а також суто для забезпечення життєво важливих інтересів суспільства (максимальне обмеження збору даних). Усі суб'єкти персональних даних мають бути повідомлені хто (орган/особа) та з якою метою отримував доступ до їх даних. Втручання має право здійснювати лише уповноважена на те законом орган/особа. Усі особи, чиї дані зазнали втручання, мусять мати ефективний механізм подання скарги до спеціального органу.	General comment No. 16 (Article 17: Right to privacy).
3.4.2. Ефективні засоби правового захисту	Держава має забезпечити осіб правом на ефективні засоби правового захисту, що можуть передбачати кримінальні, адміністративні чи цивільні процеси. Особи мають отримати можливість оскаржувати рішення чи практики у судовому порядку. Де релевантно, особи мають бути забезпечені правом на компенсацію.	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), (Article 12);

		Explanatory Report to Convention 108+ (paras. 99-100).
	Держава має забезпечити осіб правом на подачу скарги до наглядового органу, який має повідомити скаржника про результат розгляду скарги, а також можливість його оскарження в судовому порядку.	General Data Protection Regulation (Article 77) .
	Держава має забезпечити осіб правом на оскарження рішень наглядового органу у судовому порядку. Це передбачає оскарження бездіяльності органу щодо розгляду скарги або вчасного повідомлення особи про його рішення.	General Data Protection Regulation (Article 78).
	Держава має забезпечити осіб правом на судове оскарження рішень контролера або оператора.	General Data Protection Regulation (Article 79).
	Особа має мати право на компенсацію матеріальної чи нематеріальної шкоди, отриманої внаслідок порушення законодавства про захист даних. Контролер чи оператор може бути звільнений від відповідальності, якщо він доведе, що він не міг вплинути на ситуацію, що призвела до порушення. Кожен з контролерів або операторів, які брали участь у порушенні прав, несе відповідальність.	General Data Protection Regulation (Article 82).
	Накладання адміністративних штрафів за порушення у сфері захисту даних має бути ефективним, пропорційним та стримуючим. При цьому має враховуватися: ● характер, тяжкість і тривалість порушення, враховуючи мету обробки і рівень завданої шкоди; ● умисний або необережний характер порушення; ● дії, вжиті контролером або оператором для пом'якшення шкоди; ● ступінь відповідальності контролера чи оператора, враховуючи технічні і організаційні заходи; ● будь-які релевантні попередні порушення з боку контролера або оператора; ● ступінь співпраці з наглядовим органом для усунення порушення та пом'якшення наслідків; ● категорії персональних даних, на які вплинуло порушення; ● спосіб, яким про порушення стало відомо наглядовому органу, зокрема, чи повідомив про порушення контролер або обробник, і якщо так, то в якій мірі; ● дотримання заходів, призначених щодо схожих порушень;	General Data Protection Regulation (Article 83).

	• дотримання затверджених кодексів поведінки; • інші фактори, що обтяжують чи пом'якшують відповідальність. Наглядовий орган може накладати штрафи, якщо адміністративна система не має іншого механізму.	
3.5. Обмеження права на повагу до приватного життя під час воєнного стану		
3.5.1. Захист персональних даних під час війни	Додаткові обмеження, що встановлюються під час дії воєнного стану мають бути необхідними та пропорційними, а також своєчасно переглядатися державою. Такі обмеження можуть встановлюватися виключно якщо мета не може бути досягнута шляхом менш інтрузивних заходів.	European Convention on Human Rights (Article 15(1)); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 9(2)).
	Держава не може здійснювати відступів від таких прав: право на життя (крім випадків смерті внаслідок правомірних воєнних дій), заборона катування, заборона рабства і примусової праці.	European Convention on Human Rights (Article 15(2)).
	Законодавчі обмеження повинні вибірково таргетувати осіб, які охоплюються легітимною метою (наприклад, боротьба зі злочинністю). Втручання з боку держави є посиленим, якщо заходи невибірково таргетують всіх осіб та якщо обробка даних охоплює значну частину населення.	Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (para. 51).
	У випадку розширення повноважень органів додаткові гарантії повинні надаватися суб'єктам даних, як-от можливість оскаржити дії органів влади у судовому порядку, технічні заходи щодо захисту даних від несанкціонованого доступу та попередній моніторинг незалежного органу щодо доступу уповноважених органів до отриманих даних.	ECtHR, Lawless v Ireland (No. 3) (para. 38); ECtHR, Brannigan and McBride v the United Kingdom (paras. 61, 64); CJEU, C-293/12 and C-594/12 (para. 65).
	Положення щодо обмеження прав у сфері захисту даних повинні адресувати: • категорії персональних даних; • обсяг обмежень (наприклад, які права буде обмежено і на який період часу); • гарантії проти зловживань та неправомірного доступу або передачі даних (включає запровадження технічних або організаційних заходів);	General Data Protection Regulation (Article 23(2)).

	• уточнення контролера (аби суб'єкт знав, до кого звертатися у випадку обмеження); • періоди зберігання даних; • ризики правам та свободам суб'єкта даних (для оцінки пропорційності та впливу обмежень); • право на повідомлення про обмеження.	
	Закон повинен бути сформульований достатньо чітко у своїх положеннях, аби особи мали адекватне уявлення про обставини та умови, за яких контролери можуть вдаватися до будь-яких обмежень.	Guidelines 10/2020 on restrictions under Article 23 GDPR (para. 17).
3.5.2. Застосування технологій стеження під час війни	Розміщення та використання технологій стеження під час воєнного стану повинно відбуватися з урахуванням вимог Конвенції про захист прав людини і основоположних свобод під час здійснення відступів від прав згідно з пунктом 3.5.1 Методології.	European Convention on Human Rights (Article 15(1)); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 9(2)).
	Технології стеження мають застосовуватися пропорційно до рівня загрози та враховувати наявні розумні альтернативи.	ECtHR, A. and Others v the United Kingdom (para. 182).
	Технології стеження використовуються виключно для тієї мети, для досягнення якої вони були розгорнуті. Інтрузивні технології (наприклад, системи, оснащені ШІ) застосовуються виключно, якщо мета не може бути досягнута за допомогою альтернативних та менш інтрузивних засобів.	ECtHR, Lawless v Ireland (No.3) (para. 30).
	При розгортанні систем стеження з метою захисту національної безпеки закон повинен передбачити належні гарантії проти зловживань, які включають, зокрема, наявність ефективних засобів правового захисту. Закон також передбачає природу, обсяг, тривалість заходів, перелік органів, уповноважених на стеження, підстави звернення до таких заходів, механізм нагляду тощо.	ECtHR, Szabó and Vissy v. Hungary (para. 57); ECtHR, Kennedy v the United Kingdom (para. 153).

	Для забезпечення пропорційності технології стеження мають застосовуватися вибірково та таргетувати окрему/певну категорію осіб, залежно від мети звернення до заходів (наприклад, антитерористичні заходи). Відповідні уточнення повинні міститися у національному законі.	ECtHR, Szabó and Vissy v. Hungary (paras. 66-67).
	Держава має розробити належну стратегію повернення до стандартів мирного часу і згортання систем, які є надмірним втручанням у права людини і допустимі лише у воєнний час.	European Convention on Human Rights (Article 15(1)); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 9(2)).
4. ВПЛИВ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ У ЦИФРОВОМУ СЕРЕДОВИЩІ		
4.1. Загальні засади		
4.1.1. Загальні принципи регулювання у сфері ШІ	Держава має впровадити загальну правову рамку для регулювання ШІ. В межах такого регулювання мають враховуватися та закріплюватися ризико-орієнтований підхід, а саме: ● чітко визначені заборонені практики у сфері ШІ (системи, що маніпулюють свідомістю людей або вводять їх в оману для прийняття людьми нетипових рішень; системи, що експлуатують вразливості людей на основі захищених характеристик; системи соціального ранкування осіб, які можуть призвести до негативних наслідків, та системи біометричної категоризації; системи предиктивної аналітики, які ґрунтуються на профілюванні осіб; скрепінг біометричних даних з інтернету; системи біометричної ідентифікації в режимі реального часу в публічних місцях (за винятком використання в правоохоронних цілях)); ● визначені системи ШІ високого ризику (використовуються як компонент безпеки чи у сферах не заборонених практик з біометричними даними, критичної інфраструктури, освіти та професійної підготовки, працевлаштування, управління працівниками, доступу та користування основними державними та приватними послугами, правоохоронної діяльності, міграції, притулку та прикордонного контролю, здійснення правосуддя та демократичних процесів);	Artificial Intelligence Act (Articles 5-6).

	• винятки щодо систем ШІ, які за загальним правилом є високоризиковими, але у конкретному випадку не становлять значного ризику (виконують вузьке процедурне завдання; покращують результат діяльності людини; виявляють шаблони прийняття рішень або відхилення від попередніх шаблонів прийняття рішень і не призначений для заміни або впливу на вже прийняті рішення; або виконують підготовче завдання до оцінювання).	
	Держава має встановити спеціальні вимоги до високоризикових систем ШІ: • створити систему управління ризиками протягом усього життєвого циклу системи ШІ; • здійснювати управління даними, щоб набори даних для навчання, тестування та валідації були релевантними, достатньо репрезентативними та вільними від помилок; • скласти технічну документацію для демонстрації відповідності; • розробити систему таким чином, щоб уможливити її автоматично записувати події, важливі для визначення ризиків національного рівня та суттєвих модифікацій протягом її життєвого циклу; • надати інструкції щодо використання наступним користувачам; • уможливити фаховий людський нагляд; • забезпечити високий рівень точності, надійності та кібербезпеки; • встановити систему управління якістю для забезпечення відповідності; • співпрацювати з наглядовими органами та органами ринкового нагляду; • обов'язок підтримувати технічну документацію в актуальному стані.	Artificial Intelligence Act (Articles 8-21); Framework Convention on Artificial Intelligence, and Human Rights, Democracy, and the Rule of Law (Article 6-13); Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Section B); UNESCO Recommendations on Ethics of AI (paras. 25-43).
	Держава має встановити спеціальні вимоги до провайдерів моделей ШІ загального призначення: • скласти технічну документацію, включаючи процес навчання і тестування, результати оцінки; • підготувати інформацію та документацію для надання подальшим користувачам, які мають намір надалі інтегрувати модель; • дотримуватися законодавства у сфері захисту інтелектуальної власності; • оприлюднити достатньо детальний опис вмісту, який використовується для навчання моделі.	Artificial Intelligence Act (Articles 53, 55); Framework Convention on Artificial Intelligence, and Human Rights, Democracy, and the Rule of Law (Article 6-13); Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Section B);

	Детальніші вимоги мають розроблятися для моделей, які мають системні ризики: ● провести оцінку моделі, включаючи документування змагального тестування для виявлення та пом'якшення системного ризику; ● оцінка та пом'якшення можливих системних ризиків, включаючи їх джерела; ● відстеження, документування і невідкладне повідомлення про серйозні інциденти; ● належний рівень захисту кібербезпеки.	UNESCO Recommendations on Ethics of AI (paras. 25-43).
	Високоризикові системи ШІ повинні супроводжуватися вичерпними інструкціями, які дозволяють правильно інтерпретувати і використовувати результати системи. Інструкції повинні містити дані про: ● постачальника; ● характеристики системи, її можливості і обмеження (показники точності та надійності системи, ризики кібербезпеки та відомі ризики для здоров'я, безпеки чи основних прав, якість роботи щодо груп осіб для яких спроєктована система); ● вимоги до апаратного забезпечення, очікуваний термін придатності, потреби в обслуговуванні. Постачальники повинні забезпечити, щоб системи ШІ, які взаємодіють з людьми, чітко повідомляли про свою природу, якщо це не є очевидним для користувача (за винятком систем у правоохоронній сфері). Постачальники систем генеративного ШІ повинні впровадити маркування та інструменти виявлення генерованого контенту, а користувачі мають повідомляти про його природу при поширенні. Користувачі систем розпізнавання емоцій і біометричної категоризації мають інформувати інших про використання.	Artificial Intelligence Act (Articles 13, 50).
	Постачальники високоризикових систем ШІ повинні повідомляти органи ринкового нагляду про інциденти. У разі серйозних інцидентів звітування має відбутися протягом 2 днів, а про випадки, що призвели до смерті, слід повідомляти негайно, але не пізніше 10 днів з моменту їх виявлення. Після звітування постачальники повинні провести розслідування у співпраці з органами влади, при цьому уникаючи змін у системі, які можуть вплинути на оцінку причин інциденту.	Artificial Intelligence Act (Article 73).

	Штрафи за порушення у сфері ШІ мають бути ефективні, пропорційні і стримуючі (враховуючи інтереси малого та середнього бізнесу). Найсуворіші покарання не мають перевищувати 35 мільйонів євро або 7% світового річного обороту. Критерії для визначення розміру санкції включають характер і серйозність порушення, попередні порушення, розмір компанії і співпрацю з органами влади. Штрафи для постачальників моделей ШІ загального призначення не мають перевищувати 15 мільйонів євро або 3% річного світового обороту.	Artificial Intelligence Act (Articles 99, 101).
	Високоризикові системи ШІ мають відповідати вимогам щодо кібербезпеки.	Cyber Resilience Act (Article 12).
4.1.2. Оцінка впливу на права людини та управління ризиками	Держава має законодавчо встановити систему управління ризиками щодо систем ШІ з високим ступенем ризику. Розробники систем ШІ повинні провести оцінку впливу на основоположні права, який може спричинити використання такої системи перед її розгортанням.	Artificial Intelligence Act (Articles 9, 27); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 16); Digital Services Act (Article 34).
	Управління ризиками	
	Розробники повинні протягом усього життєвого циклу системи ШІ здійснювати оцінку ризиків, що включає: ● виявлення та аналіз відомих ризиків для здоров'я, безпеки або основоположних прав, коли високоризикова система ШІ використовується відповідно до її цільового призначення; ● оцінку та аналіз ризиків, які можуть виникнути, коли система ШІ діє відповідно до її цільового призначення, а також за умов обґрунтовано передбачуваного зловживання; ● оцінку інших потенційних ризиків на основі аналізу даних пост-ринкового моніторингу; ● вжиття заходів з управління ризиками. Заходи з управління ризиками повинні бути такими, щоб залишкові ризики визнавалися прийнятними. При розробці заходів має бути забезпечено: ● усунення або зменшення ризиків, наскільки це технічно можливо, за рахунок належного проектування та розробки високоризикової системи ШІ; ● впровадження заходів пом'якшення та контролю, що стосуються ризиків, які неможливо усунути;	Artificial Intelligence Act (Article 9).

	• надання інформації та навчання тих, хто розгортає системи ШІ. З метою усунення або зменшення ризиків слід приділяти увагу технічним знанням, досвіду, освіті, підготовці, які очікуються від користувачів та контексту використання системи. Під час впровадження системи управління ризиками постачальники повинні враховувати, чи може система ШІ з огляду на її цільове призначення мати негативний вплив на дітей або інші вразливі групи.	
	Оцінка впливу на права людини	
	Розробники повинні перед розгортанням системи ШІ з високим ступенем ризику провести оцінку впливу на фундаментальні права, що охоплює: • мету та контекст використання системи ШІ; • часові рамки та частоту використання; • потенційних постраждалих осіб або групи осіб; • потенційні ризики заподіяння шкоди цим групам; • заходи людського нагляду; • механізми зменшення ризиків та управління ними. Якщо під час використання системи ШІ з'ясувалося, що відбулися технічні чи організаційні зміни, може виникнути потреба проведення повторної оцінки впливу. Після проведення оцінки впливу розробник має повідомити орган ринкового нагляду про її результати. В рамках проведення оцінки впливу на права людини можуть враховуватися результати оцінки впливу на захист даних, які здійснюються відповідно до профільного законодавства.	Artificial Intelligence Act (Article 27); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 16); General Data Protection Regulation (Article 35).
	При здійсненні оцінки ризиків розробники мають залучати стейкхолдерів, які можуть зазнати особливого впливу систем ШІ, а також враховувати контекстуальні особливості застосування систем	HUDERIA Methodology (2024).
4.1.3. Фаховий людський нагляд за системами ШІ	Держава має встановити обов'язок запроваджувати належні технічні інструменти для взаємодії фахівця з системою ШІ.	Artificial Intelligence Act, (Article 14(1); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law, (Article 8); UNESCO Recommendations on Ethics of AI, (para. 35).

	Вимога фахового людського нагляду обов'язкова для систем ШІ із високим рівнем ризику.	Artificial Intelligence Act, (Article 14(2)).
	Питання «життя і смерті» не можуть вирішуватися системами ШІ без фахового людського нагляду.	UNESCO Recommendations on Ethics of AI, (para. 36).
	Фахівець, який здійснює нагляд, має мати змогу: ● розуміти можливості і обмеження системи ШІ та мати можливість контролювати її роботу, у тому числі в контексті виявлення та усунення аномалій, дисфункцій і неочікуваних результатів; ● залишатися свідомим тенденції надмірного покладання на вихідні дані, надані системою ШІ; ● правильно інтерпретувати результати роботи системи ШІ, враховуючи доступні інструменти та методи інтерпретації; ● прийняти рішення – у будь-якій конкретній ситуації не використовувати систему ШІ або іншим чином ігнорувати, скасовувати чи змінювати її результати; ● втручатися в роботу системи ШІ або переривати її роботу за допомогою кнопки «стоп» або подібної процедури, яка зупиняє систему ШІ в безпечному стані.	Artificial Intelligence Act, (Article 14(4)).
	Вимога фахового людського нагляду включає як індивідуальний нагляд за системами ШІ, так і встановлення інституційного механізму нагляду, механізмів саморегулювання (кодексів поведінки тощо). Багаторівневий процес має бути запроваджено у випадках необхідності незалежного фахового нагляду.	UNESCO Recommendations on Ethics of AI (paras. 35-36); Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (para. 5.3); Explanatory Report to Framework Convention on AI (paras. 63-65).
4.1.4. Кодекси практики та кодекси поведінки	Держава має сприяти розробці і підписанню добровільних кодексів, які можуть як встановлювати додаткові стандарти, так і пропонувати варіанти імплементації законодавчих норм.	Artificial Intelligence Act (Articles 56, 95); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 8); Explanatory Report to Framework Convention on AI (para. 63).
	Держава має сприяти розробці кодексів практики – документів, що містять тлумачення законодавчих вимог та порядок їх застосування залежно від	Artificial Intelligence Act (Article 95).

	сфери чи типу систем ШІ, до яких такі вимоги застосовні. Щонайменше, такі кодекси мають включати інформацію про: ● обов'язки провайдерів систем ШІ загального призначення та їх відповідність поточному стану розвитку технологій; ● деталі щодо того, як висвітлювати інформацію щодо тренувальних даних; ● ідентифікація системних ризиків, включно з їх джерелами; ● процедури, заходи і модальності оцінки системних ризиків, включно з документацією.	
	Держава має сприяти розробці кодексів поведінки (індивідуальних або для груп провайдерів) – документів, що передбачають додаткові зобов'язання, які на себе беруть провайдери систем ШІ поруч із законодавчими вимогами. Кодекси можуть, поміж іншого, включати такі теми: ● формування практик у сфері довірчого (trustworthy) ШІ; ● забезпечення безпеки довкілля і мінімізація ризиків у цій сфері; ● грамотність у сфері ШІ; ● забезпечення інклюзивності і різноманіття при розробці ШІ; ● захист вразливих осіб та груп осіб. Кодекси мають враховувати потреби малих гравців, включно зі стартапами.	Artificial Intelligence Act, (Article 95).
	Розробка кодексів має здійснюватися із залученням усіх зацікавлених сторін, включно з академічною спільнотою, індустрією, незалежними експертами і представниками громадянського суспільства. Кодекси можуть стосуватися одного питання чи серії різних питань.	Artificial Intelligence Act, (Articles 56(3), 95(3)).
	Провайдери моделей ШІ загального призначення можуть покладатися на кодекси практики, щоб продемонструвати дотримання вимог. Також вони можуть впроваджувати стандарти альтернативним способом, відповідність якого законодавчим вимогам перевірятиме наглядовий орган.	Artificial Intelligence Act (Articles 53(4)б 55(2)).
	При визначенні розміру і виду штрафних санкцій за порушення законодавства держава враховує (не)дотримання зобов'язань, взятих на себе суб'єктами відповідно до кодексів практики та кодексів поведінки.	Artificial Intelligence Act (Articles 101(1)).
4.1.5. Регуляторні пісочниці і	Держава має впровадити щонайменше одну регуляторну пісочницю (самостійно або в колаборації з іншими державами) – контрольоване середовище, яке сприяє інноваціям і розробці, навчанню, тестуванню (в тому числі в реальних умовах) та перевірці інноваційних систем ШІ протягом	Artificial Intelligence Act (Article 57); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 13);

тестування в умовах реального світу	обмеженого часу перед їх випуском на ринок. Інші регуляторні пісочниці можуть бути впроваджені на місцевих або регіональних рівнях.	Explanatory Report to Framework Convention on AI (paras. 92-93); UNESCO Recommendations on Ethics of AI, (para. 69).
	Держава має допомагати ідентифікувати в рамках пісочниць конкретні ризики для фундаментальних прав, здоров'я і безпеки, тестування, заходів пом'якшення наслідків і їх ефективності, зобов'язань і вимог дотримання національного законодавства. Якщо неможливо знайти заходи пом'якшення ризиків, наглядові органи можуть тимчасово призупинити участь у пісочниці чи тестування продукту. Участь у пісочницях має супроводжуватися звітом щодо результатів.	Artificial Intelligence Act (Article 57(6-7, 11)).
	Якщо діяльність в рамках пісочниць стосується обробки персональних даних, наглядом має займатися відповідний регулятор. Персональні дані, зібрані для інших цілей, можуть використовуватися в межах пісочниць для розробки і тестування систем ШІ, якщо: ● системи ШІ спрямовані на задоволення публічного інтересу (публічне здоров'я, захист довкілля, безпека транспорту тощо); ● дані не можуть бути анонімізовані, замінені синтетичними чи неперсональними даними; ● є механізми виявлення високих ризиків відповідно до Загального регламенту про захист даних (GDPR); ● персональні дані в межах пісочниці перебувають у функціонально окремому середовищі з обмеженим доступом; ● персональні дані не потрапляють за межі пісочниці без відповідних правових підстав, а їх обробка жодних чином не впливає на права суб'єктів даних; ● персональні дані мають видалятися після завершення тестування або строку їх зберігання, а активності щодо їх обробки мають чітко протоколюватися.	Artificial Intelligence Act (Articles 57(10), 59).
	Держава має розробити зрозуміле регулювання регуляторних пісочниць, включно критеріями доступу до пісочниць, процедур подачі заявок на участь у пісочницях, умов та вимог, застосовних до учасників. Участь має відбуватися на рівних умовах для будь-яких провайдерів (включно зі стартапами), а також із залученням сторонніх експертів державного і	Artificial Intelligence Act (Article 58).

	недержавного сектору. Пісочниці мають бути доступними протягом усього періоду тестування, а також надавати функціонал, необхідний для тестування, бенчмарків, оцінки і пояснення режиму функціонування систем ШІ.	
	Тестування високоризикових систем в умовах реального світу можливе, якщо: ● план щодо такого тестування надісланий наглядовому органу, який його затвердив; ● тестування в умовах реального світу належно зареєстроване; ● передача даних тестування у треті країни можлива лише якщо вони забезпечують належний рівень захисту даних; ● тестування не триває довше, ніж необхідно, і загальна тривалість не перевищує 6 місяців (може бути продовжена на додаткові 6 місяців окремим дозволом); ● вразливі групи належно захищені; ● суб'єкти, залучені до тестування, надали на це поінформовану згоду (у випадку тестування систем ШІ у сфері правопорядку – вжито заходів, щоб права суб'єктів не порушувалися). Така згода може бути у будь-який момент відкликана, що означатиме припинення тестування; ● призначено відповідальних осіб з належною кваліфікацією для нагляду за процесом тестування; ● результати роботи систем ШІ можуть бути переглянуті та скасовані. Наглядові органи мають мати змогу здійснювати нагляд за такою діяльністю, а також отримувати повідомлення про будь-які інциденти в ході такого тестування. Якщо інциденти неможливо припинити чи пом'якшити їх вплив – тестування має бути припинене. Провайдери несуть відповідальність за будь-яку шкоду, спричинену внаслідок тестування систем ШІ в умовах реального світу.	Artificial Intelligence Act (Article 60).

	Тестування високоризикових систем в умовах реального світу поза пісочницями потребує попередньої поінформованої згоди учасників такого процесу.	Artificial Intelligence Act (Article 61).
4.2. Інституції в сфері ШІ		
4.2.1. Нотифікуючий орган	Держава повинна призначити щонайменше один нотифікуючий орган, відповідальний за розробку та виконання процедур для оцінювання, призначення та повідомлення органів з оцінки відповідності та моніторингу їх діяльності. Цей орган повинен здійснювати свої повноваження незалежно, неупереджено та об'єктивно.	Artificial Intelligence Act (Articles 28(1), 70(1)).
	Держава має забезпечити, щоб компетентні органи були забезпечені достатніми технічними, фінансовими, людськими ресурсами та інфраструктурою для ефективного виконання завдань. Має бути достатня кількість персоналу, компетентного з: ● технологій ШІ; ● обробки даних; ● захисту персональних даних; ● кібербезпеки; ● основоположних прав; ● ризиків для здоров'я та безпеки; ● знання існуючих стандартів та правових вимог.	Artificial Intelligence Act (Article 70(3)).
	Призначені державою органи повинні дотримуватись правил щодо конфіденційності: ● захищаючи права інтелектуальної власності та конфіденційну інформацію, включно з комерційною таємницею; ● ефективно виконуючи вимоги законодавства щодо перевірок та аудиту; ● враховуючи інтереси громадської та національної безпеки; ● враховуючи особливості проведення кримінального або адміністративного провадження.	Artificial Intelligence Act (Article 78).
	Нотифікуючі органи мають дотримуватися правил заборони конфлікту інтересів з органами з оцінки відповідності, рішення щодо нотифікації органів	Artificial Intelligence Act (Article 28).

	з оцінки відповідності мають прийматися компетентними особами, відмінними від тих, які проводили оцінку цих органів. Нотифікуючі органи не повинні здійснювати жодної діяльності, яку здійснюють органи з оцінки відповідності або будь-яких консультаційних послуг на комерційній чи конкурентній основі.	
	Нотифікуючі органи можуть нотифікувати лише ті органи з оцінки відповідності, які задовольняють вимоги законодавства.	Artificial Intelligence Act (Article 30).
4.2.2. Нагляд за діяльністю ринку	Держава повинна призначити щонайменше один орган ринкового нагляду. Діяльність цього органу має відповідати вимогам щодо незалежності, неупередженості та ефективності, а також поважати принцип конфіденційності, описаний у пункті 4.2.1 Методології.	Artificial Intelligence Act (Articles 70(1), 78).
	Органи ринкового нагляду повинні щорічно звітувати національним органам з питань конкуренції про будь-яку потенційно важливу інформацію, в тому числі про використання заборонених практик та про вжиті заходи. Повноваження органів ринкового нагляду можуть виконувати інші спеціалізовані наглядові органи у конкретних сферах, або ж навпаки орган ринкового нагляду може виконувати повноваження ринкового моніторингу у сфері ШІ замість профільних органів. Для високоризикових систем ШІ, які використовуються для правоохоронних цілей, прикордонного контролю чи здійснення правосуддя, держави-члени призначають органами ринкового нагляду контролюючий орган у сфері захисту персональних даних або інший орган, що відповідає вимогам наведеним у пунктах 3.4.1 та 3.4.2 Методології.	Artificial Intelligence Act (Articles 74(2-6), 74(8)).
	Постачальники повинні надати органам ринкового нагляду доступ до документації, а також наборів даних для навчання, валідації та тестування високоризикових систем ШІ з високим за умови дотримання гарантій безпеки. Органу ринкового нагляду надається доступ до вихідного коду високоризикових системи ШІ за обґрунтованим запитом і якщо: ● доступ необхідний для оцінки відповідності системи ШІ обов'язковим вимогам до таких систем; ● процедури тестування або аудиту та перевірки на основі даних і документації недостатньо.	Artificial Intelligence Act (Article 74(12-13)).

	Повноваження органів ринкового нагляду мають включати: ● участь в нагляді за регуляторною пісочницею; ● можливість призупинення або припинення випробування систем ШІ в реальних умовах в разі виявлення порушень; ● можливість вимагати від постачальника змінити будь-який аспект тестування в реальних умовах.	Artificial Intelligence Act (Article 76).
	Держава повинна оприлюднити перелік органів контролю за дотриманням прав людини і підтримувати його в актуальному стані. Такі органи мають право запитувати і отримувати доступ до будь-якої документації розробників відповідно до закону.	Artificial Intelligence Act (Article 77).
	Якщо орган ринкового нагляду має підстави вважати, що система ШІ становить високий ризик, він повинен провести оцінку відповідності системи ШІ законодавству. Якщо в рамках оцінки встановлено, що система не відповідає вимогам закону, орган ринкового нагляду зобов'язує оператора системи ШІ забезпечити її відповідність закону або вилучити цю систему з ринку.	Artificial Intelligence Act (Article 79); Market Surveillance Regulation (Article 3(19)).
	Якщо орган ринкового нагляду має обґрунтований сумнів у правильності класифікації системи ШІ як невисокоризикової, він може провести повторну оцінку системи. Якщо з'ясовується, що система ШІ є високоризиковою, орган ринкового нагляду має повідомити провайдера вжити заходів для виконання обов'язків, передбачених для таких систем ШІ.	Artificial Intelligence Act (Article 80).
4.2.3. Засоби правового захисту	Держава має забезпечити, щоб будь-яка фізична або юридична особа, яка вважає, що її права та свободи порушено системою ШІ, отримала належні засоби правового захисту, як-от можливість подати скаргу до наглядового органу чи суду.	Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 14); UNESCO Recommendations on Ethics of AI (para. 55); Artificial Intelligence Act (Article 85).
	Держава має забезпечити, що будь-яка особа, що зазнала впливу рішеннями розробника системи ШІ має право звернутись для отримання обгрунтування ролі системи ШІ в прийнятті рішень. Надана інформація має бути достатньою для того, щоб особа могла оскаржити результати роботи системи ШІ або інші порушення.	Artificial Intelligence Act (Article 86(1)); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 14).
	Органи ринкового нагляду повинні встановити відповідні процедури щодо: ● подання скарг стосовно порушень законодавства;	Market Surveillance Regulation (Article 11(7)).

	• подальших дій за скаргами або повідомленнями з питань, що стосуються ризиків систем ШІ; • перевірки того, що суб'єктами вжиті необхідні коригувальні заходи (у разі потреби).	
	Держава має забезпечити, щоб юридичні особи в приватному та державному секторах встановлювали канали та процедури для внутрішньої звітності, що дозволяли б повідомляти інформацію про порушення, зокрема: • особам, які мають статус працівника, в тому числі державним службовцям; • особам, які мають статус самозайнятої особи; • акціонерам і особам, що належать до адміністративного, управлінського або наглядового органу підприємства, включаючи невиконавчих членів, а також волонтерам і оплачуваним або неоплачуваним стажерам; • будь-яким особам, які працюють під наглядом та керівництвом підрядників, субпідрядників та постачальників; • особам, які повідомляють про порушення, якщо вони повідомляють або публічно розкривають інформацію про порушення, отриману в рамках трудових відносин, які з того часу припинилися.	Whistleblower Directive (Articles 4, 8).

	Якщо внаслідок використання програмного забезпечення або продуктів з інтегрованим програмним забезпеченням) настала матеріальна чи нематеріальна шкода, особа має право на її відшкодування. Це право застосовне у випадках: • смерті або тілесних ушкоджень, включаючи медично визнану шкоду психологічному здоров'ю; • пошкодження чи знищення майна, за винятком самого дефектного продукту або продукту, пошкодженого дефектним інтегрованим компонентом, а також майна, що використовується виключно в професійних цілях; • знищення або пошкодження даних, які не використовуються в професійних цілях.	Product Liability Directive (Articles 5-6).
4.3. Контент та ШІ		
4.3.1. Вимоги щодо маркування контенту	Держава, постачальники, і користувачі мають забезпечувати достатній рівень прозорості щодо походження контенту, створеного або модифікованого ШІ.	Framework Convention on Artificial Intelligence, and Human Rights, Democracy, and the Rule of Law (Article 8); OECD Recommendation of the Council on Artificial Intelligence (para. 1.3).
	Держава повинна встановити чіткі вимоги прозорості, щоб забезпечити довіру до систем ШІ, включно з розкриттям природи згенерованого контенту.	UNESCO Recommendations on Ethics of AI (para. 70).
	Держава має забезпечити, щоб постачальники систем ШІ поважали свободу вираження поглядів і прозорість онлайн-комунікацій, та гарантували користувачам доступ до різноманітних точок зору.	UNESCO Recommendations on Ethics of AI (para. 113).
	Постачальники систем ШІ мають забезпечити, щоб системи ШІ розроблялися таким чином, щоб: • особи, що взаємодіють з системами ШІ, були поінформовані про таку взаємодію;	Artificial Intelligence Act (Article 50).

	• контент (вихідні дані), створений або модифікований системами ШІ, був промаркований в машинному форматі, аби вплив ШІ можна було виявити; • технічні рішення були ефективними, сумісними, стійкими і надійними, беручи до уваги технічні обмеження, специфіку та особливості різних типів контенту; • контент (аудіо, відео, зображення, тощо), що становить діпфейк, відповідно промаркований. Це обмеження не застосовне у випадках, що стосуються виявлення, попередження, розслідування та притягнення до відповідальності за злочини, а також у випадках, коли згенерованих контент перевірив фахівець.	
	Держава має сприяти складанню кодексів практики для сприяння ефективному виконанню зобов'язань щодо виявлення та маркування ШІ-модифікованого контенту.	Artificial Intelligence Act (Article 50(7)).
4.3.2. Протидія дезінформації	Держава має сприяти розвитку навичок цифрової та медіаграмотності для зміцнення критичного мислення та навичок, необхідних для розуміння, відповідального використання та нагляду за результатами роботи систем ШІ для протидії дезінформації.	UNESCO Recommendations on Ethics of AI (para. 114); The Strengthened Code of Practice on Disinformation (Commitment 17).
	Держава має прямо заборонити системи ШІ, що маніпулюють свідомістю людей або вводять їх в оману для прийняття людьми нетипових рішень. Держава має запобігати використанню систем ШІ для створення неправдивого контенту, розповсюдження дезінформації, введення аудиторії в оману у разі, якщо системи не є забороненими, але несуть ризики такої діяльності. Системи ШІ мають використовуватись на користь підтримки якості та цілісності інформаційного простору.	Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 8); Explanatory Report to Framework Convention on AI and Human Rights, Democracy and the Rule of Law (Article 5); OECD Recommendation of the Council on AI (para. 1.3).
	Держава має встановити обов'язок маркування згенерованого контенту та напрацювання кодексів практики у цій сфері відповідно до вимог, описаних у пунктах 4.1.4 та 4.3.1 Методології.	Artificial Intelligence Act (Article 50).
	Компанії і організації, що займаються розміщенням реклами, зобов'язуються демонетизувати поширення дезінформації, вдосконалити політики та системи, які визначають придатність вмісту для монетизації та поширення, а також впровадити засоби реагування на недобросовісне використання функції реклами та розповсюдження дезінформації.	The Strengthened Code of Practice on Disinformation (Commitment 1, 2).

	Держава повинна заохочувати онлайн-платформи складати кодекси поведінки, що передбачають ефективну передачу інформації, яка повністю поважає права та інтереси всіх залучених сторін, а також конкурентне, прозоре та справедливе середовище в онлайн-рекламі. Компанії та організації, що займаються розповсюдженням контенту, зобов'язуються вживати засоби протидії дезінформації, а саме: ● забезпечення прозорості щодо ШІ-модифікованого контенту, що допомагає користувачам відрізнити такий контент від створеного людиною; ● забезпечення того, щоб будь-який контент, який уже маркований як дезінформація, залишався таким при подальшому поширенні користувачами; ● надання інформації про критерії, за якими контент відображається користувачам, зокрема щодо рекомендаційних систем, які можуть посилювати дезінформацію; ● створення технологічних рішень для перевірки джерела та автентичності цифрового контенту; ● інтеграція інструментів фактчекінгу для підвищення точності виявлення дезінформації та співпраця з незалежними організаціями для перевірки та позначення неправдивої інформації; ● проведення регулярних аудитів щодо впровадження механізмів протидії дезінформації.	Digital Services Act (Articles 45-47); The Strengthened Code of Practice on Disinformation.
	Дуже великі онлайн-платформи повинні здійснювати оцінку ризиків щодо розповсюдження нелегального контенту та неправдивої інформації.	Digital Services Act (Article 34).
4.3.3. Вимоги до систем управління контентом	Держава має встановити вимоги до систем модерації, пріоритезації і рекомендації контенту відповідно до їх рівня ризиковості та встановити вимогу оцінки ризиків та впливу на права людини. Держава має сприяти прозорості таких систем та забезпеченню плюралізму думок внаслідок їх роботи. Провайдери платформ-брамників не мають безпідставно пріоритезувати власний контент чи власні продукти, а також мають уможливити налаштування відповідних сервісів видачі контенту (в тому числі товарів) самостійно користувачами.	Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Articles 1, 5, 10); Explanatory Report to Framework Convention on AI (paras. 18, 44, 75); UNESCO Recommendations on Ethics of AI (paras. 35-36); Digital Markets Act (Article 5).
	Держава має заборонити системи ШІ, що використовують методи впливу на підсвідомість або є умисно маніпулятивними чи оманливими і мають на меті	Artificial Intelligence Act (Article 5(1)(a));

	вплив на поведінку людини шляхом погіршення її здатності приймати обґрунтоване рішення, тим самим змушуючи приймати рішення, яке вона в іншому випадку не прийняла б і яке з високою ймовірністю завдасть істотної шкоди.	
	Держава має встановити заборону на розробку, організацію чи оперування інтерфейсами таким чином, щоб вводити в оману або маніпулювати користувачами або іншим чином суттєво погіршувати здатність користувачів приймати вільні та обґрунтовані рішення. Це може включати деталізацію запитів на прийняття користувачами рішень, повторне запитування згоди, легка процедура відмови від сервісів. Держава має зобов'язати провайдерів онлайн платформ розробити і оприлюднити умови користування, що роз'яснюють, як саме працюють системи рекомендації контенту, а також як на них можна вплинути (персоналізувати, вимкнути тощо). Вони мають включати: ● найбільш значущі критерії для визначення як відбувається видача інформації; ● причини значущості тих чи інших параметрів. Де такі системи надають декілька опцій, провайдери мають уможливити персоналізацію і налаштування систем рекомендації самостійно користувачами. Функціонал має бути зрозумілим і доступним.	Digital Services Act (Articles 25, 27).
	Держава має заборонити рекламу, що ґрунтується на профілюванні неповнолітніх.	Digital Services Act (Article 28).
	Держава має зобов'язати провайдерів онлайн-платформ вчасно реагувати на скарги щодо неправомірного контенту або контенту, що порушує умови використання. Держава має зобов'язати провайдерів великих онлайн-платформ проводити оцінки ризиків і вживати заходи для їх пом'якшення, в тому числі щодо механізмів модерації контенту, систем рекомендацій та рекламних систем.	Digital Services Act (Articles 20, 34-35).
	Держава має забезпечити право користувачів налаштовувати медіапропозицію. Це включає можливість легко змінювати налаштування пристрою або користувацького інтерфейсу, що контролює або управляє доступом і використанням медіапослуг, та адаптувати його до власних потреб. Виробники та імпортери мають забезпечити розрізнюваність	Media Freedom Act (Article 20).

	медіасервісів в рамках їх продуктів. Держава має сприяти розробці гармонізованих стандартів щодо дизайну користувацьких інтерфейсів.	
4.4. ШІ та приватність		
4.4.1. Порядок збору даних для розробки систем ШІ	Національні правила повинні передбачити належний механізм обміну даними для цілей тренування та валідації систем ШІ. Розпорядники даних зобов'язані надати доступ до відповідних даних без зайвої затримки, з такою ж якістю, яка доступна власнику даних, у легкому, безпечному, безкоштовному, комплексному, структурованому, широко використовуваному та машиночитабельному форматі. Де можливо, дані також повинні надаватися у постійному режимі та режимі реального часу.	Data Act (Article 5(1)).
	Дані можуть бути отримані лише у законний спосіб, враховуючи законодавчо передбачені підстави обробки персональних даних. Вони включають, зокрема, обов'язкову згоду суб'єкта даних, а також можливість відкликання згоди на обробку даних.	Data Act (Article 5(7)); General Data Protection Regulation (Article 6).
	Національні правила повинні встановлювати обмеження щодо доступу третіх осіб до спільних даних для захисту конфіденційності, приватності та комерційної таємниці, а також обмеження на використання даних ринковими конкурентами власника даних.	Data Act (Article 5(9,10)).
	Національні правила можуть передбачати надання доступу до даних захищених авторським правом виключно для цілей «добування даних» в межах наукових досліджень. Такий доступ супроводжується заходами безпеки та цілісності баз даних.	Directive (EU) 2019/790 (Article 3).
	Розробники систем ШІ зобов'язані обробляти отримані дані виключно для цілей тренування ШІ та за умов, погоджених із розпорядником даних. Після досягнення цілей обробки відповідні дані підлягають видаленню, якщо іншого не погоджено із розпорядником даних. Національні правила можуть передбачити додаткові обмеження щодо розпорядження отриманими даними (наприклад, заборона використання даних для цілей профайлингу).	Data Act (Article 6).
	Національні правила повинні передбачити механізм щодо повторного використання певних даних державного сектору, які не можуть бути доступні як відкриті дані. Умови повторного використання повинні бути недискримінаційними, прозорими, пропорційними та об'єктивно	Data Governance Act (Article 5).

	виправданими щодо категорій та характеру даних, для яких дозволено повторне використання. Вимоги щодо повторного використання можуть включати: ● попередню анонімізацію або модифікацію даних; ● дотримання вимог авторського права; ● отримання доступу до даних виключно в межах фізичних приміщень без можливості віддаленого (онлайн) доступу.	
	Національні правила повинні передбачити механізм «альтруїзму даних» та умови, за яких особи можуть добровільно ділитися своїми даними. Такі умови повинні супроводжуватися обов'язковими гарантіями захисту персональних даних.	Data Governance Act (Article 16).
	Національні правила повинні передбачити створення регуляторних пісочниць для тренування та валідації систем ШІ.	Artificial Intelligence Act (Article 57(5)).
4.4.2. Захист від автоматизованого прийняття рішень	Держава має забезпечити право не бути підданим автоматизованому рішенню, яке суттєво впливає на особу, без урахування її поглядів (в тому числі профайлінг). Це передбачає можливість заперечувати проти такого рішення, наводячи конкретні аргументи, а також отримувати можливість перегляду рішення автоматизованої системи. Винятками до цього правила є випадки, коли: ● автоматизоване прийняття рішень/обробка даних необхідні для укладення/виконання договору; ● автоматизоване прийняття рішень передбачене законом; ● особа надає пряму згоду на такі дії. У таких випадках, особу мають наділити правовими запобіжниками від зловживань (зокрема, можливістю людського втручання у процес прийняття рішень в критичних ситуаціях).	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), Article 9(1)(a); Explanatory Report to Convention 108+ (para. 75); General Data Protection Regulation (Articles 21-22); Guidelines on Artificial Intelligence and Data Protection (para. III(4)); Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (para. 4.3).
	Держава має забезпечити особу правом заперечувати проти обробки даних в прямих маркетингових цілях (включно з профайлінгом). Одразу після заперечення обробка даних має припинятися. Якщо дані обробляються з науковою, історичною чи статистичною метою, особа має право заперечувати проти обробки. Обробка може продовжуватися, якщо суспільний інтерес переважає над інтересами особи.	General Data Protection Regulation (Article 21).

	Держава має наділити особу правом отримувати на запит інформацію про причини того чи іншого автоматизованого рішення, результати якого впливають на цю особу (включно з профайлінгом). Так, у випадку відмови у кредитуванні на основі автоматизованої обробки заявок, особі мають пояснити, чому саме система видала відмову.	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), Article 9(1)(c); Explanatory Report to Convention 108+ (para. 77); Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (para. 4.3); Artificial Intelligence Act (Article 86).
	Держава має заохочувати імплементацію ефективних і цільових програм з медіа- та цифрової грамотності, щоб уможливити осіб розуміти технічний функціонал і обмеження систем.	Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (Preamble 7(a)).
4.4.3. Системи біометричної ідентифікації	Використання систем дистанційної біометричної ідентифікації в режимі реального часу в публічних місцях є забороненою, за винятком суворої необхідності для: ● цілеспрямованого пошуку конкретних жертв викрадення, торгівлі людьми або сексуальної експлуатації людей, а також розшук зниклих безвісти; ● запобігання конкретній, істотній та безпосередній загрозі життю або фізичній безпеці фізичних осіб, або реальній та поточній чи справжній та передбачуваній загрозі терористичного нападу; ● локалізації або ідентифікації особи, яка підозрюється у вчиненні кримінального правопорушення, з метою проведення кримінального розслідування чи переслідування.	Artificial Intelligence Act (Article 5(1)(h)).
	Обробка біометричних даних має бути обмеженою і може здійснюватися лише на чітко визначених правових підставах.	General Data Protection Regulation (Article 9(2)).
	Обробка біометричних даних може здійснюватися для цілей ідентифікації особи, яка в'їжджає/виїжджає з території країни. При цьому суб'єкт, чиї дані підлягають збору, повідомляється, зокрема, про органи, які матимуть доступ до даних, обов'язок взяття відбитків пальців та фотографування зображення їх обличчя, перелік прав, якими наділений суб'єкт даних тощо.	Regulation (EU) 2017/2226 (Articles 14(2), 50).

	Національний закон може встановлювати правила щодо механізму здійснення скринінгу («screening») осіб, яким заборонений в'їзд на територію країни. Скринінг включає, зокрема, ідентифікацію особи та реєстрацію її біометричних даних. Національний закон повинен передбачати гарантії суб'єкта даних, який підлягає скринінгу, а також незалежний наглядовий механізм для моніторингу заходів.	Regulation (EU) 2024/1356 (Articles 5(1), 8(5), 10-11).
	При обробці великих даних (які включають біометричні дані) системи повинні бути розроблені таким чином, щоб звичайні дані не розкривали чутливу інформацію. У випадку, якщо звичайні дані продовжують використовуватися для розкриття чутливої інформації, вони підлягають такому ж рівню захисту, як і чутливі дані.	Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (para. 4.4).
	Використання систем дистанційної біометричної ідентифікації в режимі реального часу в публічних місцях для правоохоронний цілей можливе виключно для підтвердження ідентифікації конкретної таргетованої особи, із врахуванням таких елементів: ● характеру ситуації, що спричиняє можливе використання, зокрема, серйозність, ймовірність і масштаб шкоди, яка була б спричинена, якби система не використовувалася; ● наслідків використання системи для прав і свобод усіх відповідних осіб, зокрема серйозність, ймовірність і масштаб цих наслідків. Використання систем дистанційної біометричної ідентифікації в режимі реального часу здійснюється з урахуванням вимог необхідності та пропорційності.	Artificial Intelligence Act (Article 5(2)).
	Використання систем дистанційної біометричної ідентифікації в режимі реального часу можливе за дозволу компетентного судового чи іншого наглядового органу, виданого після отримання обґрунтованої вимоги. Національний закон встановлює правила для вимоги, видачі та здійснення авторизації, а також подальшого нагляду та звітності таких дозволів. Правила також встановлюють для яких цілей та щодо яких кримінальних правопорушень компетентним органам може бути дозволено використовувати відповідні системи.	Artificial Intelligence Act (Article 5(3), 5(5)); Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Article 8).
	Про використання систем дистанційної біометричної ідентифікації в режимі реального часу повинні бути повідомлені відповідний орган ринкового нагляду та національний орган із захисту даних.	Artificial Intelligence Act (Article 5(4)).

	Використання систем біометричної ідентифікації (не в режимі реального часу) має відповідати вимогам щодо систем високого ризику.	Artificial Intelligence Act (Article 6(2)).
	Системи біометричної категоризації, які класифікують окремих фізичних осіб на основі їхніх біометричних даних, щоб зробити висновок про їх расову чи політичну приналежність погляди, членство в профспілці, релігійні або філософські переконання, статеве життя або сексуальну орієнтацію, повинні бути забороненими.	Artificial Intelligence Act (Article 5(1)(g)).
	Національний закон повинен встановити внутрішні правила щодо оцінки та зменшення ризиків, спричинених відповідними системами, враховуючи фактичний і потенційний вплив на права людини. Оцінка також стосується потенційної заборони щодо використання окремих систем ШІ, якщо вони несумісні з правами людини.	Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Article 16(1), 16(4)).
4.4.4. Приватність за проєктуванням і приватність за замовчуванням	Держава має впровадити вимоги приватності за проєктуванням (англ. «privacy-by-design») та приватності за замовчуванням (англ. «privacy by default»).	Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (para. 3.2); Guidelines on AI and Data Protection (para. I(2)); UNESCO Recommendations on Ethics of AI (para. 34); Artificial Intelligence Act (Preamble 69).
	Приватність за проєктуванням передбачає фокус на дотриманні стандартів на етапі розробки систем ШІ шляхом впровадження технічних та організаційних заходів, як-от псевдонімізації. Приватність за замовчуванням стосується налаштування інтерфейсу так, щоб захист приватності завжди був опцією за замовчуванням, зокрема у питанні обробки мінімальної кількості персональних даних, тривалості обробки даних, строку зберігання та доступності даних. Тобто потрібно дати активну згоду на те, щоб будь-які надмірні дії вчинялися щодо персональних даних. Держава може розробити механізм сертифікації для підтвердження дотримання вимог щодо приватності за проєктуванням та приватності за замовчуванням.	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), (Article 10); Explanatory Report to Convention 108+, (para. 89); General Data Protection Regulation (Articles 25).
4.5. ШІ та заборона дискримінації		

4.5.1. Збалансованість наборів даних	Держава зобов'язана впровадити заходи щодо забезпечення рівності, включно з гендерною рівністю, на всіх етапах життєвого циклу систем ШІ, а також заборони дискримінації. Це включає вимоги до усунення стереотипів з боку розробників та постачальників систем, збір якісних та неупереджених даних, заходи щодо попередження дискримінації при застосуванні систем ШІ, надмірне покладання на системи ШІ, що посилює упередження тощо. Упередження і помилки у наборах даних мають своєчасно і належним чином виправлятися. Держави мають забезпечити право на ефективні засоби правового захисту в контексті порушення рівності системами ШІ.	Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Articles 10, 17); Explanatory Report to Framework Convention on AI (paras. 75-76); UNESCO Recommendations on Ethics of AI (paras. 29, 90); Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (paras. C(1.4, 3.1-3.2)).
	Тренувальні, тестові та валідаційні дані для систем ШІ мають відповідати вимогам щодо: ● вибору дизайну системи ШІ; ● процесу збору даних і походження даних, вибору підстав збору персональних даних; ● анотації, маркування, фільтрування, оновлення та агрегації даних відповідно до стандартів; ● формулювання припущень щодо того, що вимірюють і репрезентують дані; ● оцінки доступності, кількості та сталості наборів даних; ● оцінки потенційних упереджень і їх впливу на права людини; ● заходів для зменшення або видалення упереджень; ● ідентифікації прогалин у наборах даних та заходів для їх усунення. Набори даних мають бути збалансовані, репрезентативні, наскільки можливо – позбавлені помилок і повні відповідно до мети, а також враховувати географічні, контекстуальні, поведінкові і функціональні умови роботи. Обробка чутливих даних можлива, якщо: ● виявлення та виправлення упереджень не можуть бути ефективно виконані шляхом обробки інших даних, включаючи синтетичні або анонімні дані; ● чутливі дані підлягають технічним обмеженням щодо повторного використання даних, заходам безпеки і збереженню конфіденційності;	Artificial Intelligence Act (Article 10); UNESCO Recommendations on Ethics of AI (para. 76).

	• відбувається контроль і документування доступу, щоб уникнути неправомірного використання; • чутливі дані не можуть передаватися іншим сторонам; • чутливі дані видаляються після виправлення упереджень або завершення періоду зберігання. Держава має заохочувати створення наборів даних, що стануть «золотим стандартом» у питаннях репрезентативності даних, надійності та правомірності отримання даних.	
	Держава має заохочувати регулярне тестування, оцінку, звітування і аудит відповідно до стандартів повноти, актуальності, конфіденційності, захисту даних, інших прав людини, рівності та безпеки на всіх етапах життєвого циклу систем ШІ. Така оцінка також має бути частиною процесів закупівель.	Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (paras. B(2.2, 3.3-3.4)).
	Держави мають формувати регуляторні органи у сфері рівності таким чином, щоб вони мали експертизу для оцінки систем ШІ та їх впливу на рівність.	Resolution 2343 (2020), Preventing discrimination caused by the use of AI (paras. 3-4, 10.1-10.3); UNESCO Recommendations on Ethics of AI (para. 74).
4.5.2. Системи предиктивної аналітики	Держава має встановити заборону на оцінку поведінкових особливостей осіб за допомогою ШІ, яка ґрунтується на обробці чутливих категорій даних і не має під собої розумної підозри у вчиненні особою злочину, а також не має людського нагляду. Заборона має охоплювати: • випуск на ринок або використання систем ШІ для оцінки або класифікації осіб або груп осіб на основі їхньої соціальної поведінки або відомої, припущеної чи передбаченої характеристики особистості, якщо така оцінка спричиняє: шкідливі наслідки для осіб у соціальних контекстах, які не мають відношення до контекстів збору даних; шкідливі наслідки, які є невиправданими або непропорційними соціальній поведінці осіб чи її тяжкості; • випуск на ринок або використання систем ШІ для оцінки або прогнозування ризику вчинення особою злочину виключно на основі профілювання особи або оцінки її особистісних якостей та характеристик (не охоплює системи ШІ, що використовують для оцінки	Artificial Intelligence Act (Article 5(1)(c-d).

	залученості особи до кримінальних дій на основі об'єктивних фактів, які можна перевірити).	
	Держава не має покладатися на процеси автоматизованого прийняття рішень у правоохоронній сфері, включно з профайлінгом, які призводять до негативних правових наслідків для особи чи суттєво впливають на неї, якщо такі процеси не передбачають належних гарантій і запобіжників від зловживань.	Law Enforcement Directive (Article 11).
	Держава має сприяти тому, щоб розробники та постачальники предиктивних систем ШІ залучали до процесів розробки, тестування та оцінки (на рівні консультування) незалежних експертів, громадянське суспільство та представників академічної спільноти.	Guidelines on Artificial Intelligence and Data Protection (para. II(6)).
	Держава має оцінювати ризики впровадження систем предиктивної аналітики та встановлювати запобіжники або альтернативні способи оцінки/реалізації прав та обов'язків.	Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (Preamble, paras. 8, 11).
	При впровадженні предиктивних систем ШІ держава має враховувати можливість упереджень у змінних чи індикаторах, особливо коли це стосується етнічної, расової чи гендерної складової. З огляду на це, держава має: ● реєструвати усі системи ШІ, що використовуються у публічному секторі з предиктивною метою; ● регулярно здійснювати оцінку впливу на права людини з фокусом на вплив систем на вразливі та маргіналізовані групи; ● пересвідчитися, що процеси прийняття рішень є зрозумілими і пояснюваними для користувачів; ● забезпечити доступність судового перегляду результатів роботи таких систем ШІ.	Resolution 2342 (2020)1, Justice by algorithm – The role of AI in policing and criminal justice systems (para. 9).
4.5.3. Портали для зворотного зв'язку	Держава має зобов'язати розробників та користувачів систем ШІ проводити аналіз заходів, вжитих для забезпечення реагування на ризики, в тому числі механізмів внутрішнього управління та інструментів для скарг. Портали для зв'язку мають бути легкодоступними і надавати можливість не лише залишати скарги, а і пропонувати, як покращити сервіси і продукти.	Artificial Intelligence Act (Article 27(1)); Recommendation CM/Rec(2020)1 of the CoM to member States on the human rights impacts of algorithmic systems (para. 4.2).

	Держава має встановити обов'язок для провайдерів онлайн-платформ оприлюднювати деталі щодо внутрішніх механізмів для скарг в умовах користування сервісом. Такі портали мають бути дружніми до користувача та сприяти надходженню деталізованої інформації щодо проблеми. Поміж іншого, портал для скарг має надати можливість оскаржити рішення про: ● видалення чи обмеження доступу до контенту; ● видалення чи призупинення діяльності акаунту; ● припинення чи призупинення надання сервісів; ● припинення чи призупинення монетизації. Провайдери онлайн-платформ мають вчасно повідомляти результати розгляду скарг і можливість їх оскарження у разі потреби, а також вчасно виправляти помилки у разі, якщо скарги обґрунтовані. Скарги мають розглядатися у недискримінаційній манері. Провайдери онлайн-платформ також можуть вживати заходів у разі зловживань порталами для скарг, в тому числі вдаючись до призупинення можливості надсилати скарги конкретними користувачами. Такі заходи мають бути пропорційними до поведінки користувачів.	Digital Services Act (Articles 14, 20, 23).
	Держава має забезпечити користувачів можливістю скаржитися на порушення їхніх прав компетентним наглядовим органам або відновлювати порушені права у судовому порядку.	Artificial Intelligence Act (Article 85); General Data Protection Regulation (Articles 12(4), 77); Framework Convention on AI, and Human Rights, Democracy, and the Rule of Law (Article 14(2)); Explanatory Report to Framework Convention on AI (para. 100).
5. ПРАВО НА ВІЛЬНІ ВИБОРИ: ПОЛІТИЧНА РЕКЛАМА В ЦИФРОВОМУ СЕРЕДОВИЩІ		
5.1. Прозорість політичної онлайн-реклами		

Законодавство має гарантувати належний рівень прозорості онлайн політичної реклами, зокрема шляхом надання інформації про замовників таких матеріалів на сервісах, де вона розміщується.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 7); The Strengthened Code of Practice on Disinformation (Commitment 8); Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 2.1).
Законодавство має містити зобов'язання для провайдерів політичної реклами щодо збереження архівів онлайн політичної реклами протягом достатнього часу у машиночитному форматі для забезпечення належного аналізу матеріалів державними інституціями та дослідниками.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 9); The Strengthened Code of Practice on Disinformation (Commitment 10, 11); Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 2.3 – 2.4); UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach (Article 115).
Законодавство має містити вимоги до маркування онлайн політичної реклами, завдяки якому у чіткий, виразний та недвозначний спосіб громадяни можуть відділити політичну рекламу від іншої реклами, дізнатися про її замовників, отримати інформацію про те, чи застосовувалися інструменти таргетингу, а також, у разі якщо ця політична реклама є елементом передвиборної агітації чи агітації на референдумі – інформацію про той виборчий чи референдумний процес, якого вона стосується.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 11); The Strengthened Code of Practice on Disinformation (Commitment 6);

	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach (Article 138).
Законодавство має передбачити обов'язок платформ періодично звітувати про суму доходів отриманих частково або повністю в обмін на надані послуги онлайн політичної реклами, у тому числі щодо використання методів таргетингу, агрегованих за кампаніями.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 14).
Законодавство має зобов'язати платформи та сайти, на яких розміщуються матеріали онлайн політичної реклами мати механізми, які дозволять фізичним або юридичним особам повідомляти їх, якщо конкретна політична реклама, опублікована ними, порушує права та свободи людини, а також суперечить Конституції та законодавству конкретної держави.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 15).
Законодавство має передбачити можливість компетентних державних інституцій витребувати у провайдерів онлайн політичної реклами будь-яку необхідну інформацію – така інформація має бути повною, точною та достовірною та надаватися у чіткому, послідовному, зведеному та зрозумілому форматі.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 16).
Законодавство має забезпечити за допомогою засобів спільного регулювання, щоб онлайн-платформи надавали доступ до політичної реклами у справедливий та недискримінаційний спосіб і встановлювали для усіх однакові ціни за однакові послуги.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Articles 2.7, 6.4).
Слід забезпечити, щоб алгоритми, що використовуються державними та приватними суб'єктами для ранжування та показу онлайн політичної реклами, а також алгоритми, що застосовуються в практиках модерації контенту були прозорими та такими, що піддаються перевірці, особливо щодо потенційної упередженості та неточностей систем, які використовуються. Держави в рамках спільного регулювання повинні встановити належний рівень прозорості алгоритмічних систем, щоб забезпечити їхню відповідність міжнародним стандартам прав людини, зокрема Рекомендації CM/Rec(2020) Комітету міністрів Ради Європи державам-членам щодо впливу алгоритмічних систем на права людини.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 4.1).
5.2. Фінансування онлайн політичної реклами	

У разі, якщо законодавство держави передбачає обмеження витрат на передвиборну агітацію, слід, де це можливо, розглянути можливість адаптації законодавства щодо лімітів витрат для політичних партій, кандидатів та відповідних політичних акторів, щоб такі ліміти також ефективно застосовувалися до цифрового середовища та його відмінних моделей функціонування та цінових моделей порівняно з агітацією у традиційних медіа.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 3.2).
Законодавство має містити заборону або суттєве обмеження іноземних пожертв та витрат на онлайн політичну рекламу. Крім того, державам слід заборонити або обмежити розмір пожертв з анонімних джерел на неї.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 3.3).
5.3. Захист виборців від недобросовісних практик таргетингу та незаконної обробки персональних даних	
Споживачам політичної реклами має бути забезпечений належний доступ до інформації щодо застосування до них таргетингу, який може використовуватися лише у разі надання прямої згоди на обробку персональних даних з цією метою.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Articles 18, 19); Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 5.2).
Держава повинна вимагати від онлайн-платформ створення інструментів, які дозволять громадянам відмовитися від політичної реклами в Інтернеті.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 5.3).
Споживачам політичної реклами має бути надане належне право на оскарження змісту та порядку розміщення політичної реклами, як шляхом створення відповідних механізмів провайдерами політичної реклами, так і через наділення відповідними повноваженнями незалежних регуляторних органів.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 24).

Законодавство має передбачити належні санкції за порушення у сфері онлайн політичної реклами – водночас важливо забезпечити, щоб такі санкції були пропорційними, аби онлайн-платформи не вдавалися до надмірних заходів, які можуть призвести до обмеження законного контенту та невиправданого втручання у право на свободу вираження поглядів.	Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising (Article 25); Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 1.4).
Платформи в рамках спільних регуляторних механізмів повинні запровадити запобіжні заходи для гарантування доброчесності послуг (дії проти ботів і фейкових акаунтів), а також протидіяти викривленню інформації та навмисному поширенню політичної дезінформації, забезпечуючи при цьому повну повагу до верховенства права та стандартів прав людини, викладених у Конвенції та інших відповідних документах Ради Європи, зокрема права на свободу вираження поглядів, гарантованого статтею 10 Конвенції, на анонімність і конфіденційність приватних комунікацій. Для забезпечення дотримання цієї вимоги держави повинні вимагати від онлайн-платформ впровадження систем прозорості для чіткого маркування автоматизованих облікових записів і дій, щоб ці дії не можна було сплутати з людською взаємодією.	Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns (Article 4.2 – 4.3).
5.4. Потенційне впровадження інтернет-голосування	
Наміри виборця не повинні залежати від системи голосування або будь-якого іншого неправомірного впливу.	Протокол до Конвенції про захист прав людини і основоположних свобод (стаття 3); Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (Appendix I, Article 3.10).
Електронне голосування має бути організоване таким чином, щоб забезпечити дотримання таємниці голосування на всіх етапах процедури голосування. Процес електронного голосування, зокрема етап підрахунку голосів, має бути організований таким чином, щоб унеможливити відновлення зв'язку між незапечатаним голосом та виборцем. Голоси є і залишаються анонімними.	Протокол до Конвенції про захист прав людини і основоположних свобод (стаття 3); Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (Appendix I, Article 4.19).

Якщо канали дистанційного е-голосування не є загальнодоступними, вони мають бути лише додатковим та необов'язковим засобом для голосування.	Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (Appendix I, Article 1.3).
5.5. Використання інструментів ШІ у виборчих процесах з дотриманням прав людини	
При впровадженні інструментів ШІ у виборчий процес має враховуватися їх вплив на права людини. Усі ці процеси мають відповідати стандартам прав людини, з огляду на те, що будь-які системи ШІ, які застосовуються у виборчому чи референдному процесі вважаються «системами високо ризику».	Artificial Intelligence Act (Article 6 (2), ANNEX III 8.2).

2025

Лабораторія
цифрової
безпеки

МІЖНАРОДНИЙ
ФОНД
ВІДРОДЖЕННЯ