



Co-funded by the  
European Union

# European Fundamental Values in Digital Era

ERASMUS-JMO-2022-HEI-TCH-RSCH  
ERASMUS-JMO-2022-COE — Jean Monnet Actions in the field of  
Higher Education: Centres of Excellence

Project: 101085385 — EFVDE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

## Workshop for practitioners (no 2)



Co-funded by the  
European Union

## Європейські фундаментальні цінності в цифрову еру

Воркшоп для практиків є частиною проекту Центр Досконалості Жана Моне “Європейські фундаментальні цінності в цифрову еру”, 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, що фінансується Європейським Союзом.

Однак висловлені погляди та думки належать лише авторам і не обов’язково відображають погляди Європейського Союзу чи Європейського виконавчого агентства з питань освіти і культури (EACEA). Ні Європейський Союз, ні орган, що надає гранти, не можуть нести за них відповідальності.



Co-funded by the  
European Union

Воркшоп для практиків  
**«Іновації європейського законодавства в сфері обороту даних»**

*27 та 28 вересня 2023*

Workshop for Practitioners  
**«Innovations in European Legislation in the Field of Data Transfers  
and Circulation»**

*September 27 and 28, 2023*



European  
Fundamentation Values  
in Digital Era



## Оборот даних для систем штучного інтелекту: пропозиції та практика в ЄС

VII ХАРКІВСЬКИЙ МІЖНАРОДНИЙ ЮРИДИЧНИЙ ФОРУМ  
Воркшоп для практиків  
“Новачії європейського законодавства в сфері обороту даних”  
27 та 28 вересня 2023

Юлія Разметаєва



Co-funded by  
the European Union

✉ [yu.s.razmetaeva@nlu.edu.ua](mailto:yu.s.razmetaeva@nlu.edu.ua)

✉ [cledt@nlu.edu.ua](mailto:cledt@nlu.edu.ua)

# Дані як ресурс для ШІ



## Цифровий суверенітет

Наприклад, EU — US обміни даними

## Повторне (вторинне) використання даних

Наприклад, the European Commission launched the European Health Data Space (EHDS) [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2711](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711)

## Різноманітність даних

Наприклад, machine learning



Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final

В обох актах немає жорсткого дуалізму між персональними та неперсональними даними, характерного для GDPR

# Дані для GAI

Незважаючи на те, що підходи Європейської комісії, позиція Ради Європейського Союзу і позиція Європейського парламенту значно збігаються, вони розходяться щодо того, як мати справу з моделями, які знаходяться на стадії обговорення/тестування

Наприклад, ChatGPT (як ШІ загального призначення)

Варіанти:

- (1) Галузеве регулювання без загальної основи
- (2) Загальна основа (Європейська Комісія, структура)
- (3) Балансування іновацій, ділитися знаннями (Рада)
- (3) Збільшити вимоги до GAI в будь-якому виді регулювання та/або запровадити окрему категорію ризику (Європарламент)

Право «не бути суб'єктом рішення, заснованого виключно на автоматизованій обробці, включно з профілюванням, яке створює юридичні наслідки щодо нього чи неї або подібним чином істотно впливає на нього чи неї»

(1) прийняте рішення (2) ґрунтується виключно на автоматизованій обробці або профілюванні та (3) має або юридичні наслідки, або аналогічні значні наслідки для суб'єкта даних.

Наприклад, 26 січня 2023 року відбулося відкрите усне слухання у справі С-634/21 (інтерпретація ст. 22 GDPR)

# Дані для надмірного втручання



## (1) чутливі та біометричні дані

Наприклад, 4 липня 2023 року Європейський суд з прав людини виніс перше рішення щодо використання розпізнавання облич

## (2) надмірна концентрація даних

Наприклад, дані, накопичені завдяки IoT





Co-funded by  
the European Union

EFVDE

European  
Fundamental Values  
in Digital Era



Європейські фундаментальні цінності у цифрову еру,  
Центр Досконалості Жана Моне

101085385 - EFVDE - ERASMUS-JMO 2022-HEI-TCH-RSCH

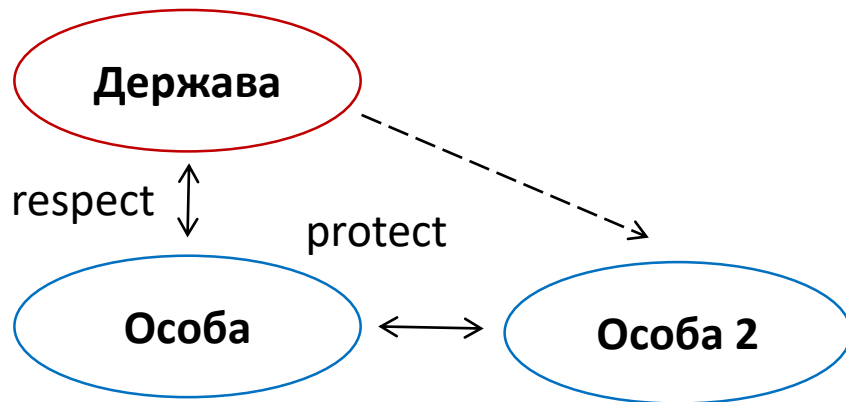
# Захист персональних даних в ЄС: зміна парадигми

Петро Сухорольський

Корені права особи на захист персональних даних – негативні права (*право на приватність, право на повагу до честі і гідності, право на недискримінацію*)

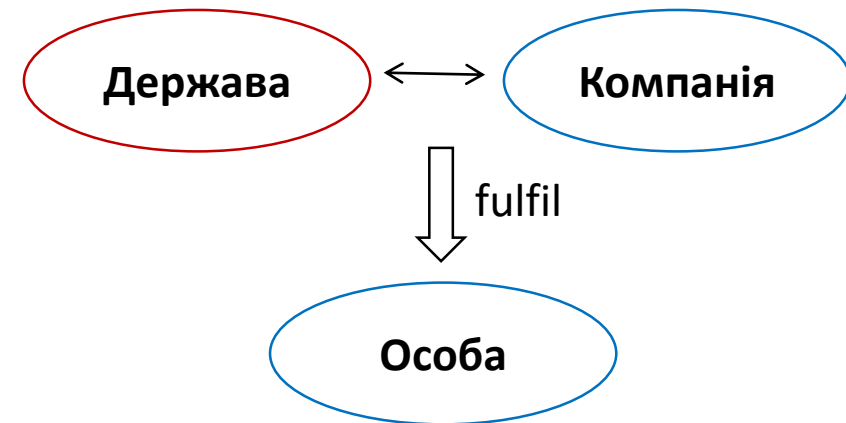
### Негативні права

*Право на приватність  
Право на гідність  
Право на недискримінацію  
Свобода вираження*



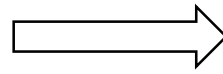
### Позитивні права

*Право на освіту  
Право на працю  
Право на медичне обслуговування*

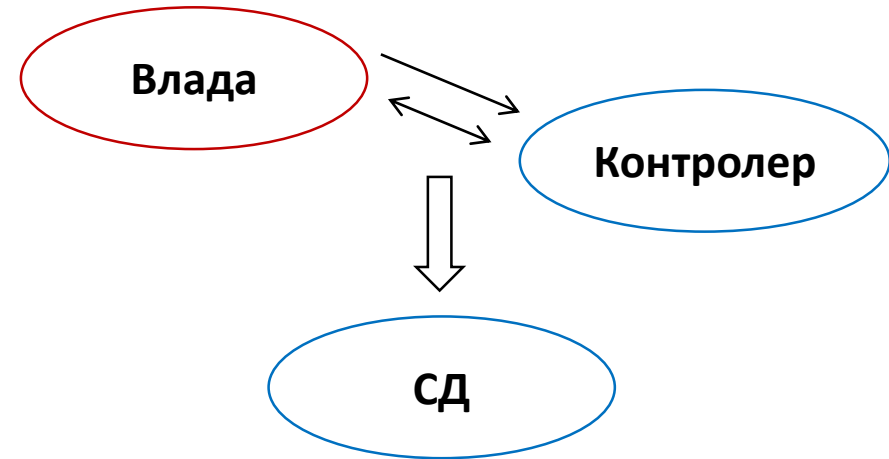
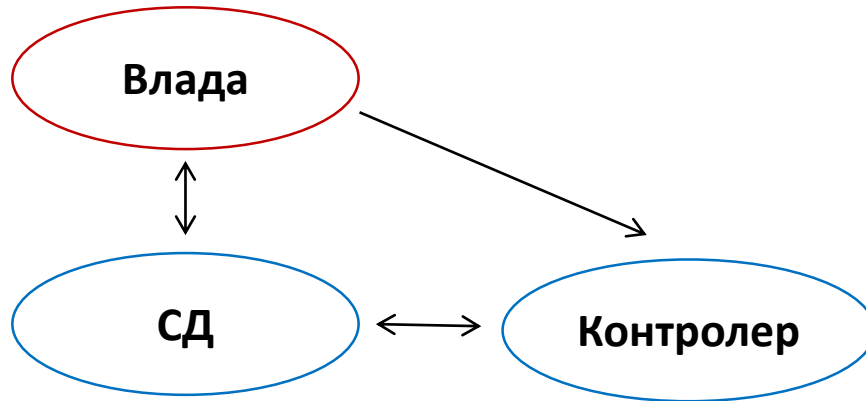


# Право на захист персональних даних

Акцент на права суб'єкта даних (СД) у відносинах з контролерами



Взаємодія влади з контролерами щодо забезпечення прав СД



Складність і недостатність прозорості аналітики великих даних може вимагати **переосмислення ідей особистого контролю персональних даних**. Слід пристосовуватися до певного соціального та технологічного контексту з урахуванням недостатньої обізнаності з боку людей. Отже, захист даних стосовно великих даних повинен здійснюватися з урахуванням ширшого поняття контролю над використанням даних, згідно з яким **індивідуальний контроль перетворюється на більш складний процес множинних оцінок впливу ризиків, пов'язаних з використанням даних**.



## Чому право на захист ПД не могло стати негативним правом людини?

- 1) Загальна тенденція «позитивізації» негативних прав;
- 2) Специфічні для права на захист ПД чинники:

складність

непрозорість

висока конкуренція

The New York Times

OPINION  
DAVID BROOKS

### A Theory of Elon Musk's Maniacal Drive

Sept. 21, 2023



Elon Musk at 3. Archivo GBB/contrasto/Redux

*Людей надихають ідеї, але ідея загальна,  
абстрактна і вузькоспрямована, а при її реалізації  
виявляється багато неочікуваних моментів*

Голосовий помічник  
Самокерований транспорт



вимагають для  
ефективної роботи  
майже необмежену  
кількість різних типів ПД

- Чи було на етапі ідеї припущення, що їх треба розглядати в контексті проблеми Старшого Брата?
- Чого очікувати від майбутніх технологій, наприклад, від нейроінтерфейсу?

## Приклад віртуальних голосових помічників

*(Guidelines 02/2021 of the European Data Protection Board on Virtual Voice Assistants)*

### Множинність суб'єктів даних

- registered users
- non-registered users
- accidental users
- multiple users for one VVA (colleagues, in a family, at school)
- different types of users (an adult, a child, an elder or a disable person)

### Складність екосистеми

### Множинність типів даних

- primary data (account data, voice recordings, requests history)
- observed data (device data that relates to a data subject, activity logs, online activities)
- inferred or derived data (e.g. user profiling)
- VVAs may have full access to the requests' content (e.g. a search engine, an online shop or a music streaming service)

### Множинність опрацювання

- VVA provides services or features and is connected to other devices or services managed by other parties
- involve automated means and human means
- specificities of the vocal interface

### Складні умови користування

### Множинність контролерів

- VVA provider (or designer)
- VVA application developer
- integrator
- owner
- third-party processor

### Множинність цілей

- executing requests
- improving machine learning model
- biometric identification
- profiling for personalized content or advertising
- unforeseen purposes etc.

## Складність

*The Cost of Reading Privacy Policies by Aleecia M. McDonald and Lorrie Faith Cranor (2008)*

«Якщо б кожен користувач в США читав кожен документ щодо правил користування ресурсами в інтернеті, то в сумі було б затрачено час, що дорівнює в середньому **244 години на рік на одного користувача** (близько 30 повних робочих днів), і цей час можна оцінити загальною сумою **\$781 мільярдів** (приблизно ВВП Туреччини у 2008)».

*European Data Protection Board*: «To create the account, users have to read and accept a **30 pages long privacy policy**. ... The information provided by the VVA designer in this case should not be deemed as concise and its complexity reduces the required transparency. Therefore, the VVA designer would not be complying with the transparency requirements as set out in Articles 12 and 13 GDPR».

## Непрозорість

- *Guidelines 02/2021* “The user might be not sufficiently informed how and by whom their data is processed”

- **Чорнокоробкова природа** сучасних технологій

- *Рішення ЄСПЛ Klass and Others v. Germany*:

*«людина може, за певних умов, стверджувати, що стала жертвою порушення, що сталося внаслідок самого факту існування таємних заходів, або законодавства, що допускає таємні заходи, без необхідності стверджувати, що такі заходи насправді застосовувалися до неї»*

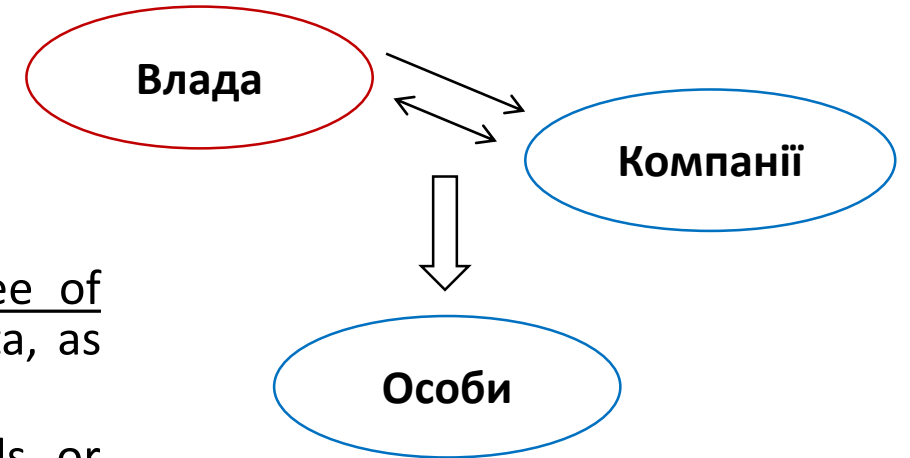
- справа *Захаров проти Росії*: ЄСПЛ формулює критерії, які він враховує, коли з'ясовує, чи людина стала жертвою порушення ст. 8 лише внаслідок самого існування системи спостереження та відповідного законодавства

## Взаємодія влади та контролерів щодо забезпечення прав СД

*Guidelines 4/2019 of the European Data Protection Board on Article 25 Data Protection by Design and by Default*

### Key design and default fairness elements may include:

- **Autonomy** – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing.
- **Non-exploitation** – The controller should not exploit the needs or vulnerabilities of data subjects.
- **Consumer choice** – The controller should not “lock in” their users in an unfair manner.
- **Power balance** – Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures.
- **No risk transfer** – Controllers should not transfer the risks of the enterprise to the data subjects.
- **No deception** – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.



***Data protection by design***

***VS***

***Data harvesting and utilization by design***

## Deceptive design patterns

### Overloading

Continuous prompting  
Privacy Maze  
Too Many Options

### Skipping

Deceptive Snuggness  
Look over there

### Stirring

Emotional Steering  
Hidden in plain sight

### Obstructing

Dead end  
Longer than necessary  
Misleading action

### Fickle

Lacking hierarchy  
Decontextualising  
Inconsistent Interface  
Language Discontinuity

### Left in the dark

Conflicting information  
Ambiguous wording or information

**Маніпулятивний патерн безперервного стимулювання** виникає, коли користувачів спонукають надати більше персональних даних, ніж необхідно для цілей обопрацювання, або погодитися на інше використання їхніх даних шляхом неодноразових запитів надати додаткові дані або погодитися з метою обробки. Такі повторювані запити можуть надходити через один або кілька пристроїв. **Користувачі, швидше за все, здадуться, оскільки вони втомилися відмовляти** в запиті кожного разу, коли вони використовують платформу.

# Стратегічний форсайт – сценарії



1. **Business as usual** – бізнес виконуватиме все складніше і складніше приписи і все більше вкладатиме ресурсів в compliance.
2. **Добровільні стратегії** – система деградуватиме під тиском власної складності і суперечностей, все більше добровільних стратегій для бізнесу.
3. **Ліберальна реакція** – раціональна чи вибухова.

# Огляд новацій європейського законодавства і проектів змін у сфері обороту даних

*Н.Ю. Філатова-Білоус  
к.ю.н., доцент кафедри цивільного судочинства,  
арбітражу і міжнародного приватного права*

# Попередні дискусії в ЄС



- Дані – це не лише персональні дані, а й неперсональні дані (відкриті дані, статистичні, дані, що генеруються при використанні IoT тощо)
- Ідея встановлення режиму власності щодо даних (А. Меркель в одній зі своїх промов у 2017 р.) і розробки «Цивільного кодексу для даних»
- Ідея створення режиму виключних прав на дані ("Building European Data Economy" (COM(2017) 9 final))



# Чинна Європейська стратегія щодо даних (COM/2020/66)



- Для забезпечення конкурентоспроможності європейського цифрового ринку необхідно створити єдиний європейський ринок даних, де дані є достатньо захищеними і водночас доступні для повторного використання іншими суб'єктами
- FAIR data principles – data shall be findable, accessible, interoperable and re-usable
- Не може існувати власності на дані і т.п.
- Суб'єкти персональних даних повинні мати інструменти і засоби для того, щоб керувати своїми даними (MyData Movement)



# Що вже зроблено?



- **General Data Protection Regulation (GDPR) 2016/679**



- **Regulation (EU) 2018/1807 on the free flow of non-personal data**

- **Directive (EU) 2019/1024 on open data and the re-use of public sector information**



# Що ще треба зробити?



**Забезпечити оборот даних,  
що не охоплені існуючим  
законодавством**

**Data Governance Act  
(2022/868)**

**Data Act  
(COM/2022/68)**



# Data Governance Act

## Вертикальні відносини щодо даних



# Що регулює?

- Повторне використання (re-use) даних, якими володіють публічні органи влади (крім відкритих даних).

*Приклад: Французька компанія DAMAE Medical надає для використання масиви зображень структури тканин шкіри для дослідження проблем і патологій шкіри*

- Засади діяльності посередників даних (data intermediaries) у ЄС

*Приклад: французька компанія DAWEX, яка дозволяє користувачам пропонувати для продажу масиви даних і придбавати масиви даних*

- Діяльність з надання даних для загальносуспільного блага (data altruism)

*Приклад: Smart Citizen – платформа, що дозволяє користувачам обмінюватися даними про рівень шуму в певних місцевостях*

- Засади передання даних до третіх країн (не членів ЄС)



# Повторне використання



- Стосується виключно даних, що перебувають у володінні публічних органів влади
- Публічні органи не зобов'язані надавати дані для повторного використання, але якщо надають, то повинні дотримуватися вимог Регламенту
- Заборонено укладати договори, що надають контрагенту публічного органу ексклюзивне право на використання даних
- Умови надання даних для повторного використання повинні бути опубліковані й доведені до загального відома
- Основний принцип надання даних для повторного використання - 'as open as possible, as closed as necessary'
- Держави-члени ЄС повинні створити єдину базу доступу до даних - платформу, через яку різні суб'єкти можуть звертатися із пропозиціями щодо надання їм даних для повторного використання



# Посередники даних



- Маркетплейси даних, пули даних та посередники, що надають суб'єктам персональних даних послуги з управління їх даними у відносинах з контролерами даних
- Посередники даних повинні повідомити уповноважені органи відповідної держави-члена ЄС про початок своєї діяльності в ЄС
- Посередники повинні дотримуватися низки вимог (не використовувати дані для власних цілей, не змінювати дані, отримані від користувачів, попереджувати будь-які несанкціоновані виливи даних і т.ін.)
- Для контролю за дотриманням цих вимог кожна держава ЄС має створити компетентний орган



- Створення реєстру організацій альтруїстів даних і визначення вимог до їх діяльності
- Встановлення меж щодо передання даних до третіх країн – дані, отримані для повторного використання, не повинні передаватися, якщо це суперечить законодавству ЄС
- Штрафи за порушення Регламенту встановлюються державами ЄС на національному рівні

# Data Act

## Горизонтальні відносини щодо даних



# Що регулює (забезпечує)?



- Можливість користувачів різних продуктів отримувати доступ до даних, згенерованих під час такого використання, і передавати ці дані третім особам  
*Приклад: власник смарт-холодильника має право на доступ до даних, згенерованих під час його використання (про покупки, тривалість зберігання продуктів і т.ін.)*
- Виключення можливості існування права інтелектуальної власності на масиви даних
- Механізми захисту користувачів від несправедливих умов договору (як для споживачів, так і для підприємців)
- Можливість перезавантажувати дані з одного хмарного сервісу на інший без зайвих обмежень і витрат
- Застосування смарт-контрактів для надійного зберігання і передання даних



# Право на доступ

- Виробник (продавець) продукту має надати користувачу інформацію про умови генерації даних, їх використання та можливість отримання доступу до даних
- Володілець даних має передати дані на вимогу користувача будь-якій визначеній ним третій особі
- Володілець даних не може укладати з третіми особами договори про передання їм виключних прав на дані користувача
- Ціна за передання даних третім особам має бути розумною, її розрахунок - прозорим

# Неможливість привласнення даних

- Положення Директиви 96/9/ЄС про бази даних, які стосуються права sui generis на бази даних, не розповсюджуються на масиви даних, які отримані внаслідок використання продукту користувачем і згенеровані автоматично

# Захист від несправедливих умов

Умови договору щодо даних є несправедливими, якщо:

- Вони суттєво суперечать добрій комерційній практиці та принципам добросовісності та справедливості
- Вони встановлені в договорах приєднання, що пропонуються особами, що володіють даними
- Особи, що приєднуються до таких договорів, є не тільки споживачами, а й малими й середніми підприємствами (SME)



# Перевантаження даних між хмарними сервісами

- Надавачі хмарних сервісів повинні усунути будь-які технічні, організаційні, юридичні та інші перешкоди до того, щоб їх користувачі могли перевантажувати свої дані до інших хмарних сервісів



# Вимоги до застосування смарт контрактів

- Надійність – смарт контракт повинен бути складений таким чином, щоб уникати функціональних помилок і маніпуляцій з боку третіх осіб
- Безпечне розірвання і призупинення – смарт контракт повинен мати механізм для припинення його функціонування
- Можливість архівування даних – у разі припинення дії смарт контракт повинен архівувати інформацію про всі дії, здійснені в рамках його виконання
- Контроль доступу – смарт контракт має бути захищеним через контрольні механізми



Co-funded by the  
European Union

Ці матеріали підготовлені командою проєкту Центр Досконалості Жана Моне “Європейські фундаментальні цінності в цифрову еру”. Матеріали є частиною проєкту Центр Досконалості Жана Моне “Європейські фундаментальні цінності в цифрову еру”, 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, що фінансується Європейським Союзом.

Однак висловлені погляди та думки належать лише авторам і не обов’язково відображають погляди Європейського Союзу чи Європейського виконавчого агентства з питань освіти і культури (EACEA). Ні Європейський Союз, ні орган, що надає гранти, не можуть нести за них відповідальності.

Ви можете зв’язатися з нами за адресою [yu.s.razmetaeva@nlu.edu.ua](mailto:yu.s.razmetaeva@nlu.edu.ua)



Co-funded by the  
European Union

The training materials were prepared by the project team of The Jean Monnet Center of Excellence European Fundamental Values in Digital Era. The materials are the part of the project The Jean Monnet Center of Excellence European Fundamental Values in Digital Era, 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

You can contact us [yu.s.razmetaeva@nlu.edu.ua](mailto:yu.s.razmetaeva@nlu.edu.ua)