Cyber crimes, ITC crimes or cyber harms?

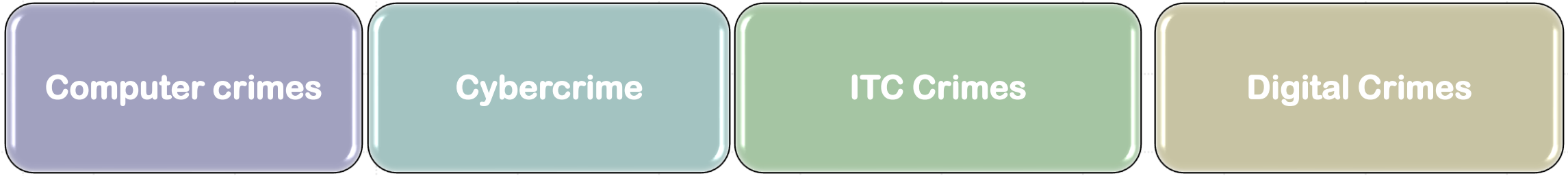
Prof. Dr. Fernando Miró Llinares

Unicri, March 2025

B) Many names and many different phenomena

90s	2000-2015	2015-2020	2020s
First personal computers	Web 1.0 and 2.0	Smartphone	Crypto, IA, Metaverse
Crimes of damage and access to data and systems	Cyberfraud, Cyber grooming	Ciber Bullying, IoT Crimes	Artificial intelligence and metaverse
Computer crimes	Cybercrime	ITC Crimes	Digital Crimes

A single correct name?



The important thing is to understand what each one implies

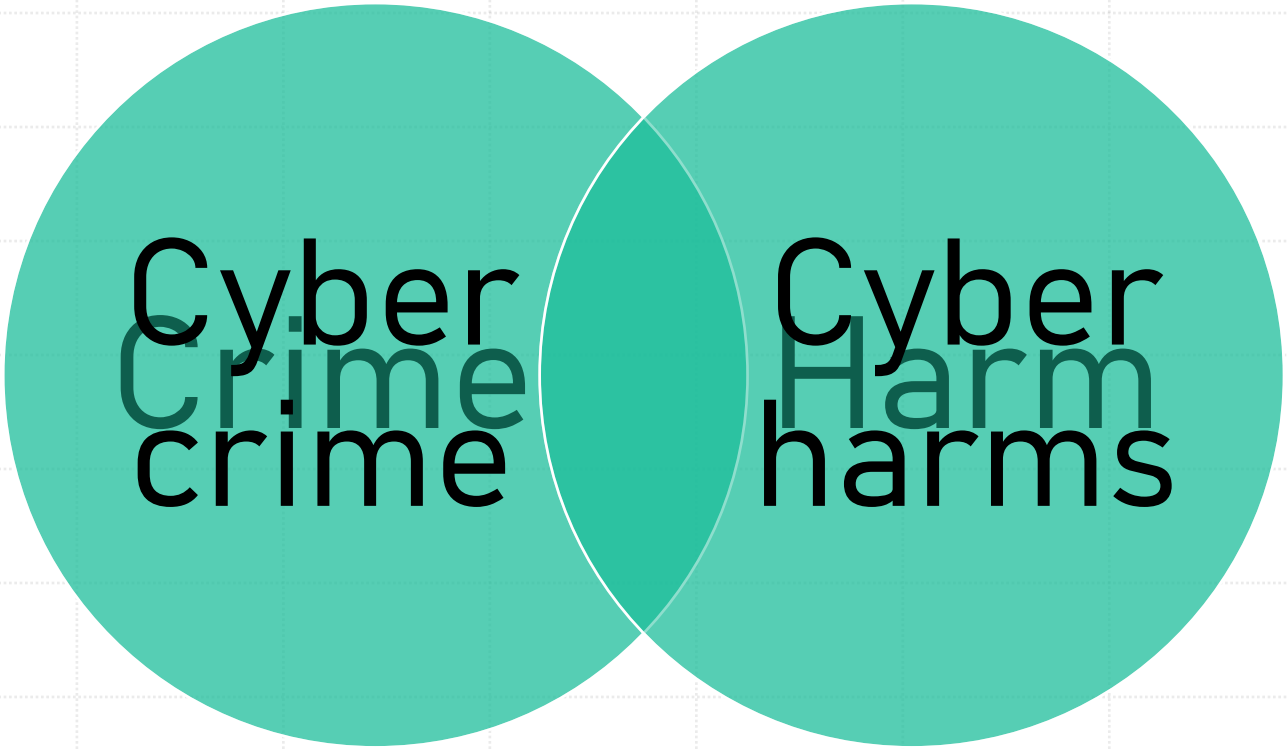
Cyber crimes, ITC crimes or cyber harms?

Prof. Dr. Fernando Miró Llinares

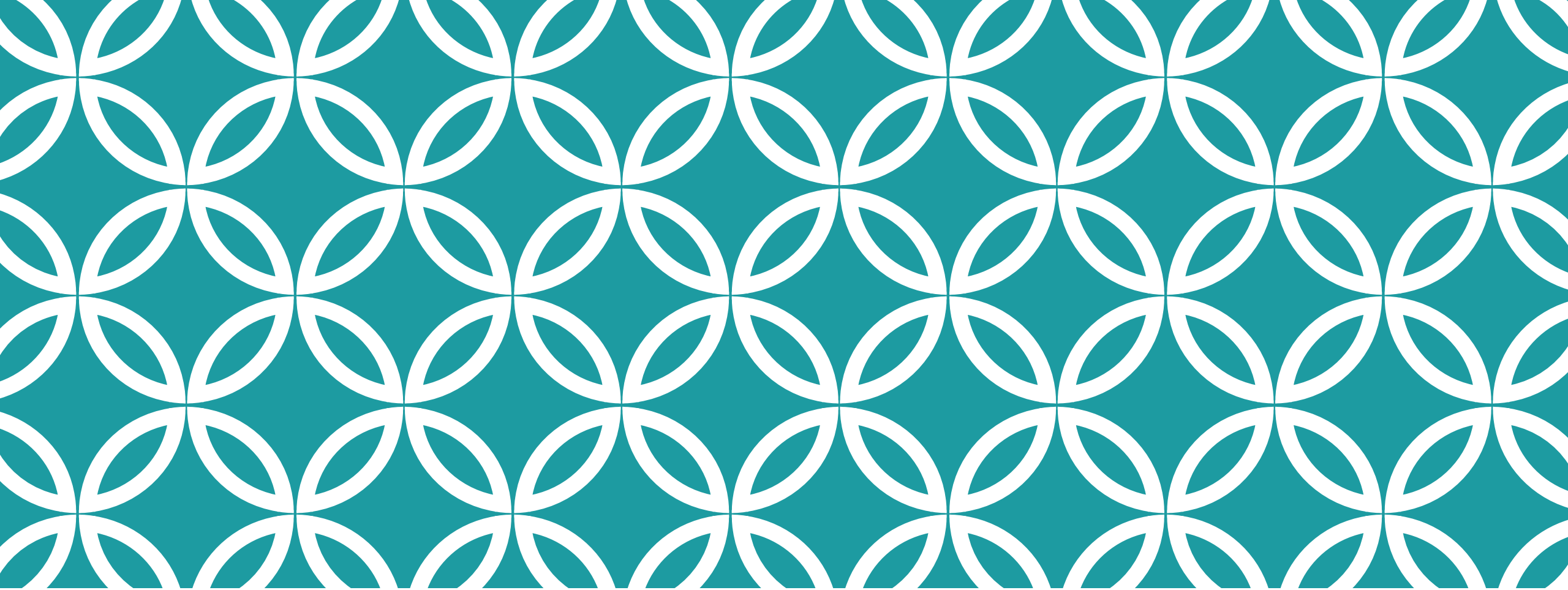
Unicri, March 2025

Should social sciences investigate phenomena like these even though they are not criminal offenses in many countries today?

- Sharing sexual images between minors
- Offensive expressions against women on social media
- Loot boxes and other forms of monetization
- Investments in cryptocurrencies with a high level of risk
- Sexual deepfakes of adults


Cyber crime
Cyber Crime
Cyber harms
Harm

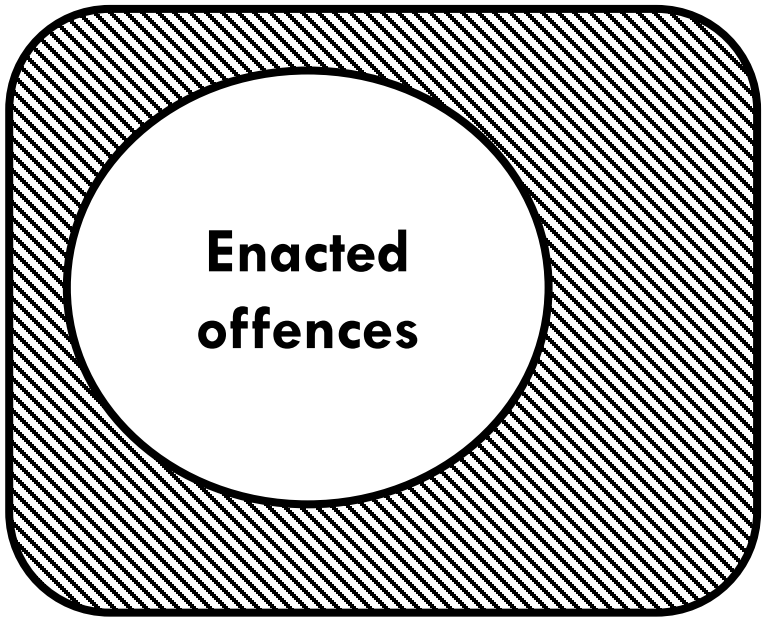
INDEX



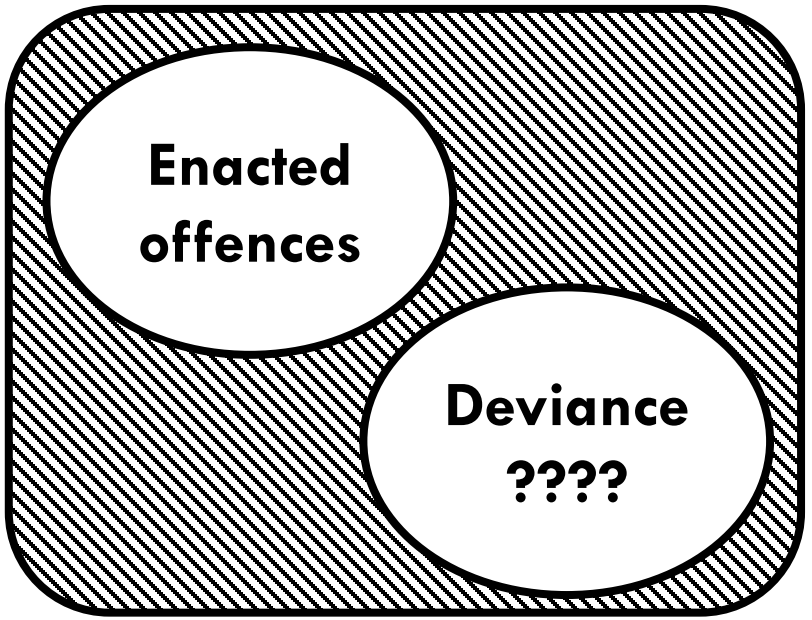
1. THE THEORETICAL RELEVANCY OF THE CONCEPT OF HARM

THE OBJECT OF CRIMINOLOGY

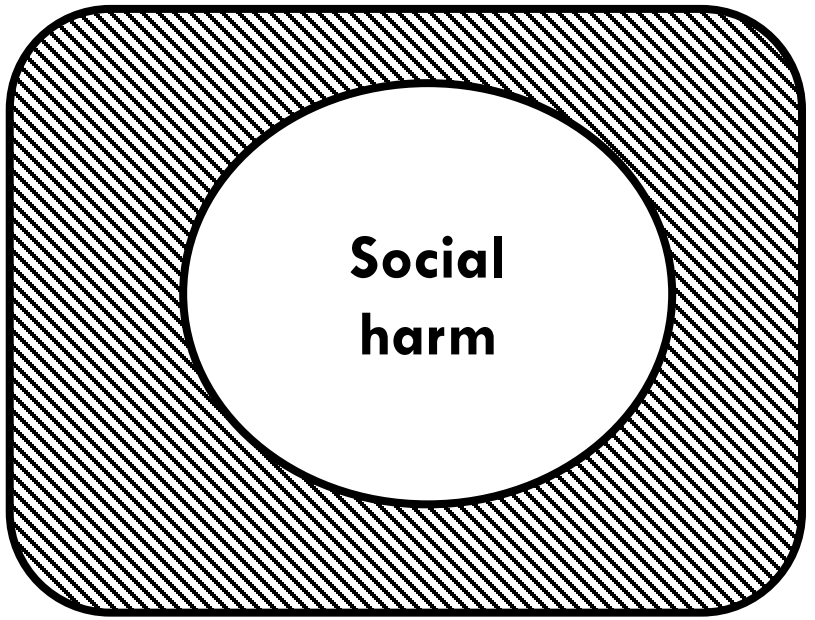
Criminal law



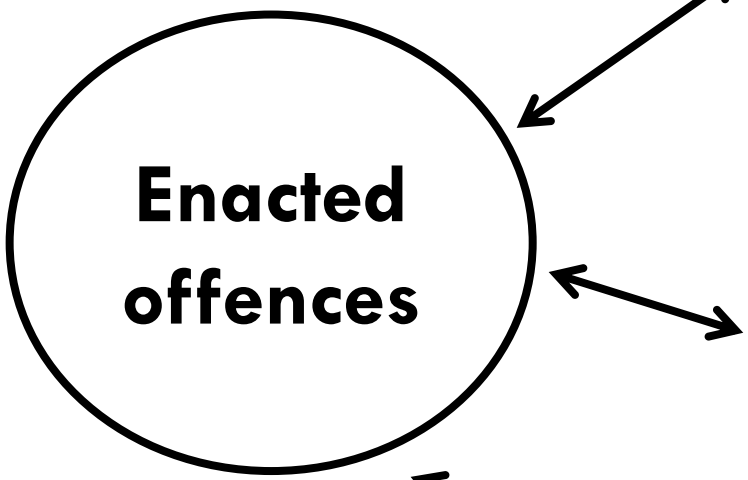
Criminology



Zemiology



IS A LEGALISTIC APPROACH ENOUGH?



Does encapsulate all the behaviours that criminology shall study? (gambling, prostitution, minor forms of online deviance)

Does guide legislators and scholars in defining what shall be criminalized?

Does inform resource allocation by law enforcement?

A LEGALISTIC APPROACH AND CYBERCRIME

LEGALISTIC APPROACH →

Shall criminology study pathological gambling online, disinformation or artificial intelligence?

Shall criminal law enact pathological gambling online, disinformation or artificial intelligence as an offence?

Is the enforcement of this hypothetical laws a priority¿?

→ ???

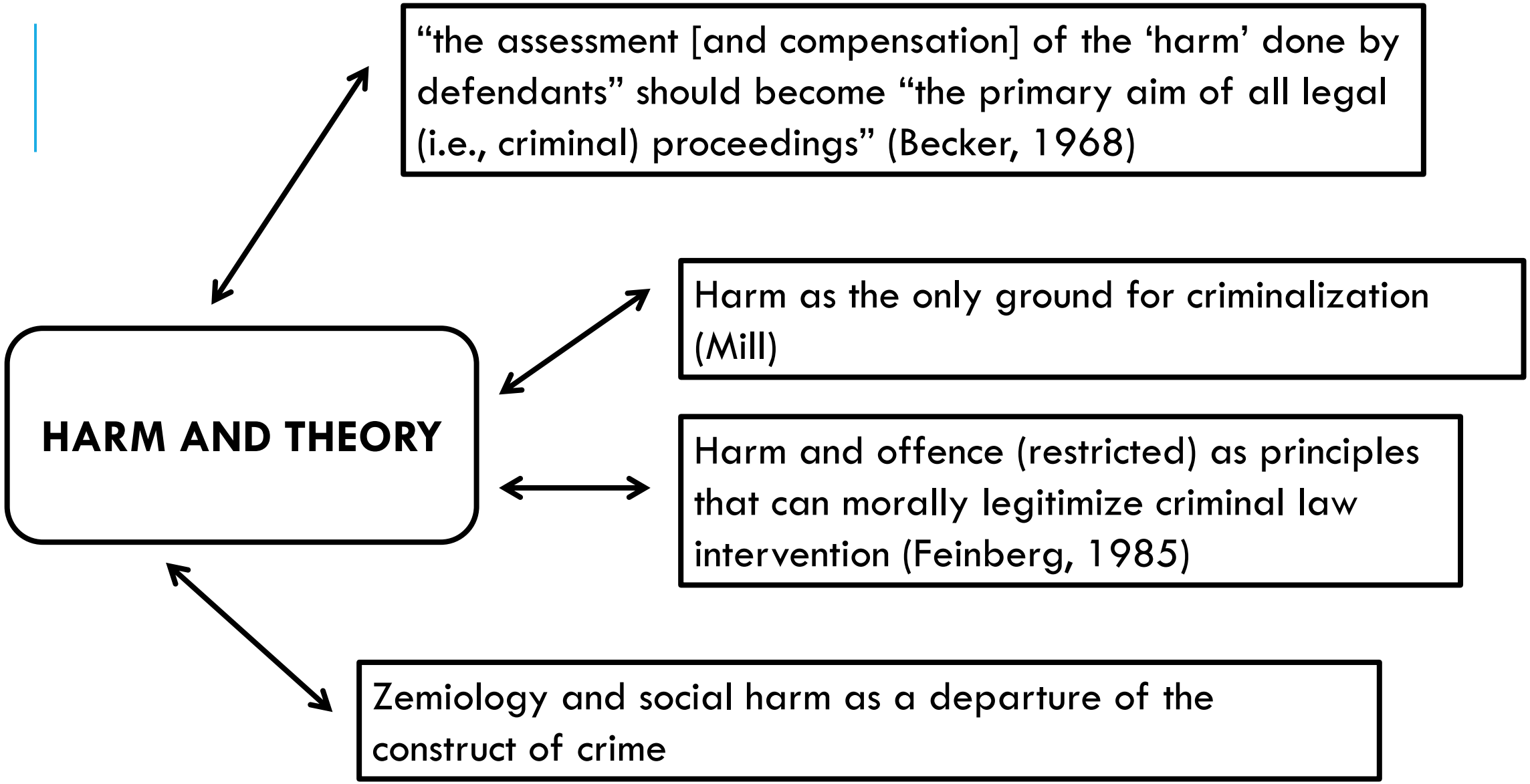
THE GOAL OF THE CONCEPT OF HARM

Why we need harm?: “a firm analytical foundation for establishing priorities and allocating resources among them” (Greenfield and Paoli, 2023)

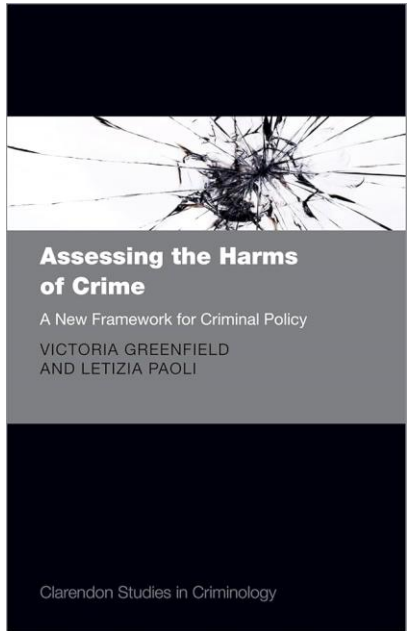
CRIMINALIZATION

CRIME CONTROL AND POLICY

SENTENCING, ASSIST VICTIMS…


"the assessment [and compensation] of the 'harm' done by defendants" should become "the primary aim of all legal (i.e., criminal) proceedings" (Becker, 1968)
HARM AND THEORY
Harm as the only ground for criminalization (Mill)
Harm and offence (restricted) as principles that can morally legitimize criminal law intervention (Feinberg, 1985)
Zemiology and social harm as a departure of the construct of crime

HARM ASSESMENT FRAMEWORK (GREENFIELD AND PAOLI, 2023)



UNDERSTAND CRIME BUSINESS

IDENTIFY HARMS AND BEARERS

ASSESS SEVERITY OF HARMS

PRIORITAZING HARMS

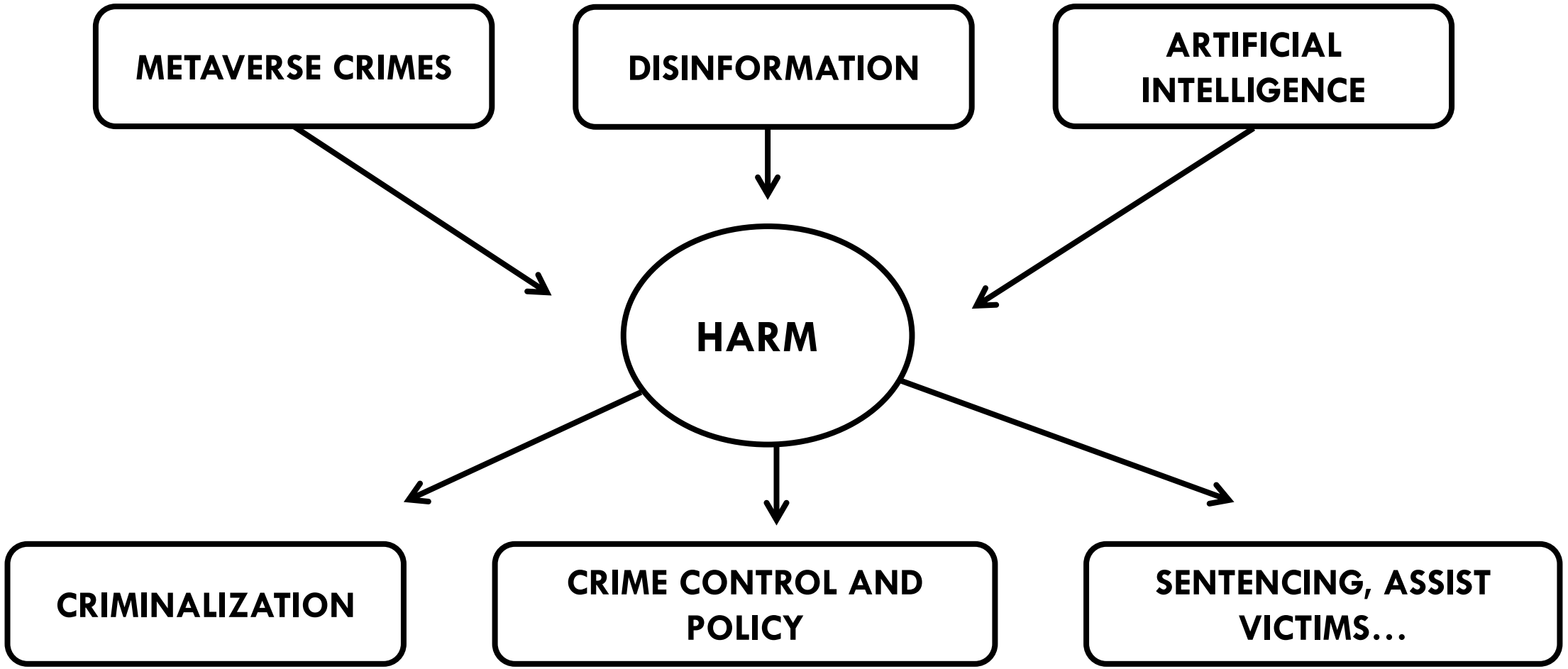
ASSESSING CAUSALITY

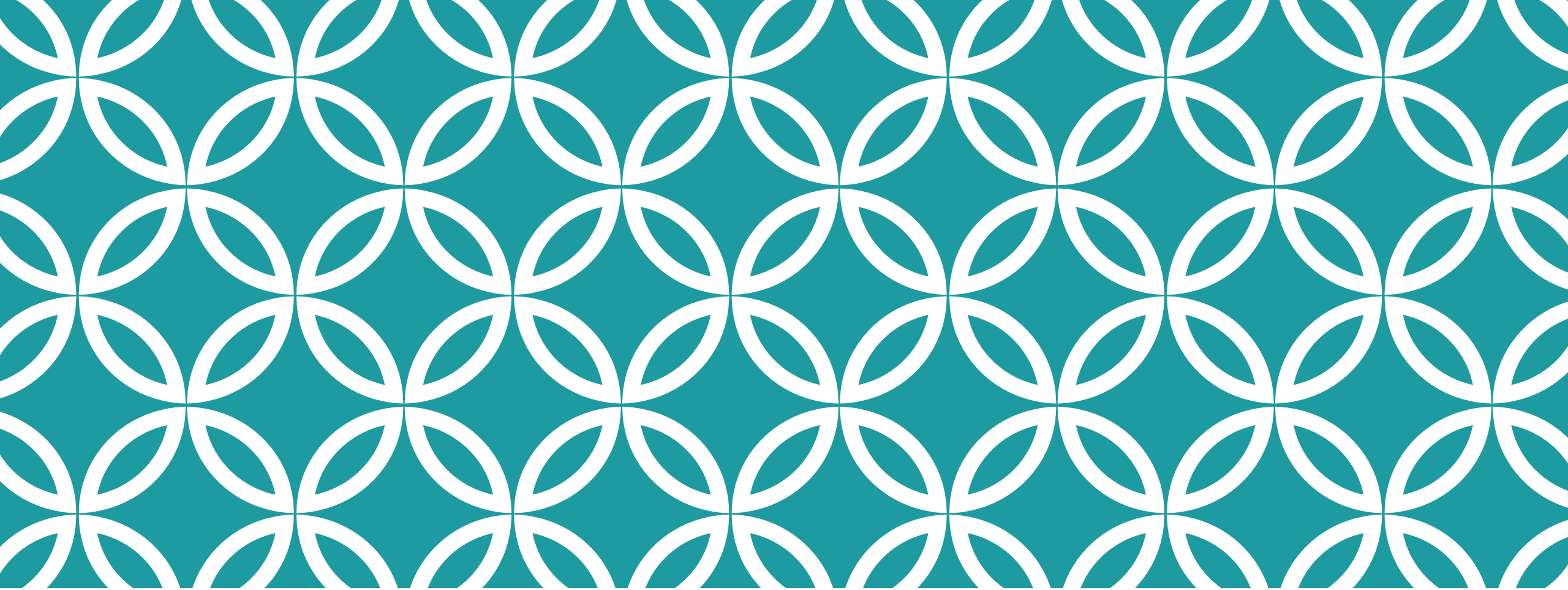
Harm = a setback to a rightful stakeholder's legitimate interests

Harms	Bearers
Functional integrity	Individuals
Material support	Private-sector entities
Reputation	Government
Privacy and autonomy	Social and physical environment

Source: Greenfield and Paoli (2023)

WHY STUDY CYBERCRIME TRENDS ON THE VIEW OF HARM?



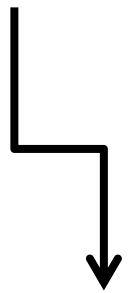


2. THE TRUE METAVERSES OF GAMING

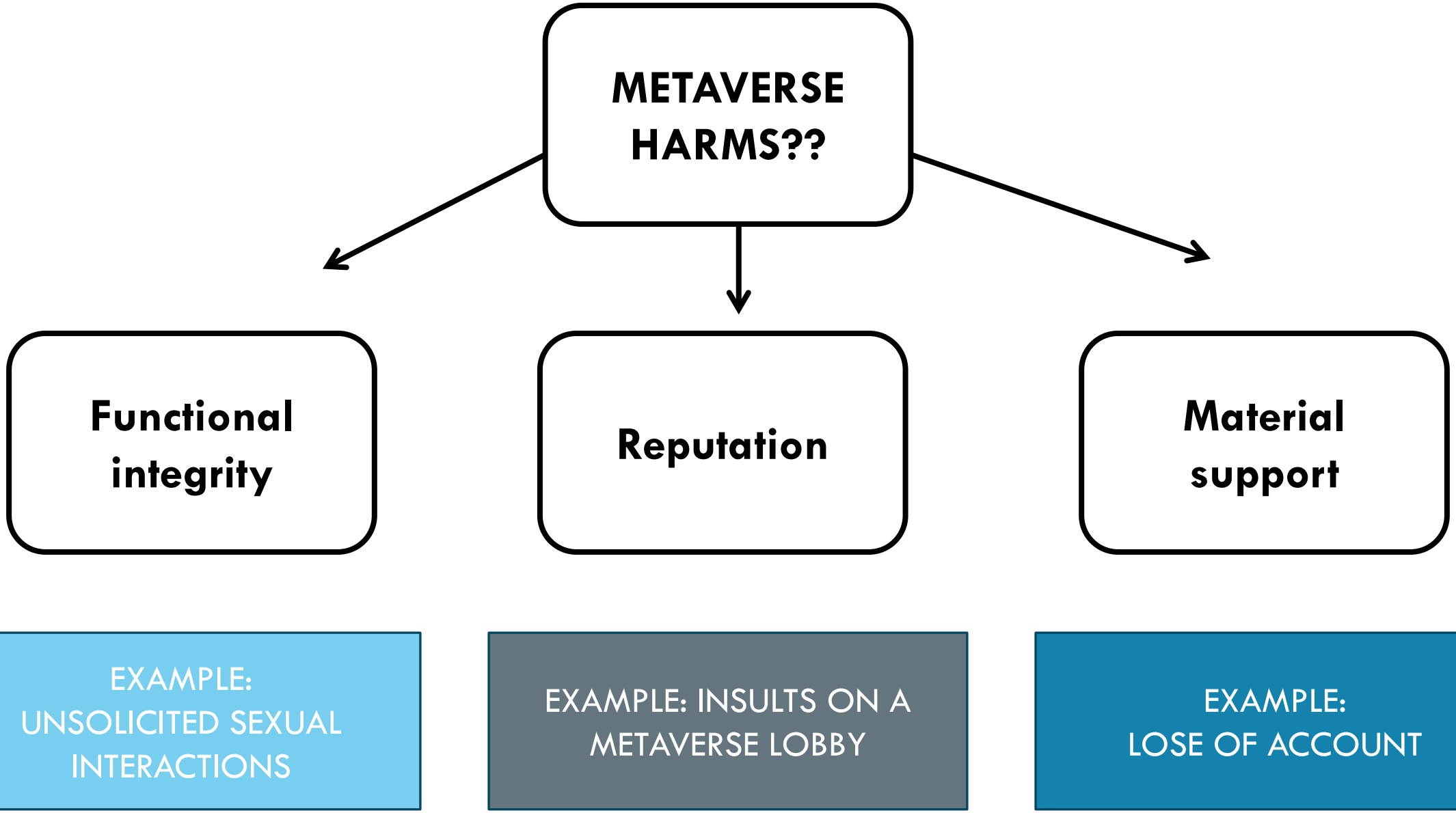
THE PROMISE OF THE METAVERSE…

AN INTERACTIVE WORLD ENABLED BY VR AND AR

- Real time convergence
- 3D world, first person camera
- More immersion trough virtual reality (VR) and Aumented reality (AR)
- Acquisition of cyber property and NFT



Harms????


METAVERSE HARMS??
Functional integrity
Reputation
Material support
EXAMPLE: UNSOLICITED SEXUAL INTERACTIONS
EXAMPLE: INSULTS ON A METAVERSE LOBBY
EXAMPLE: LOSE OF ACCOUNT

THE METAVERSE AS A CEO DREAM…

Is going to be the Metaverse a part of our routine activities?

Does really the Metaverse bring something new?

DOES REALLY THE METAVERSE BRING SOMETHING NEW? THE CASE OF MULTIPLAYER GAMES

THE RICH ECOSYSTEM OF GAMING

Use and industry data: 53% of Europeans play video games (VideogamesEurope, 2023); private sector data states that there are 3.42 billion players worldwide in 2024 and that the industry will rise $187.7 billion (Newzoo, 2024)

Game diversity: Single player and multiplayer (cooperative, shooter games, battle royal, multiplayer battle arena); console games and mobile games

Adjacent communities: 136,624 watch playing League of Legends weekly in Twitch and 127,250 GTAV (Twitch Tracker, 2025); an influencer economy linked to gaming profitable by brands (influencer advertisement)

CONNVERGENCE IN CYBERPLACES

Single player:
User to developer interactions

Multiplayer:
User to developer and user to user interactions

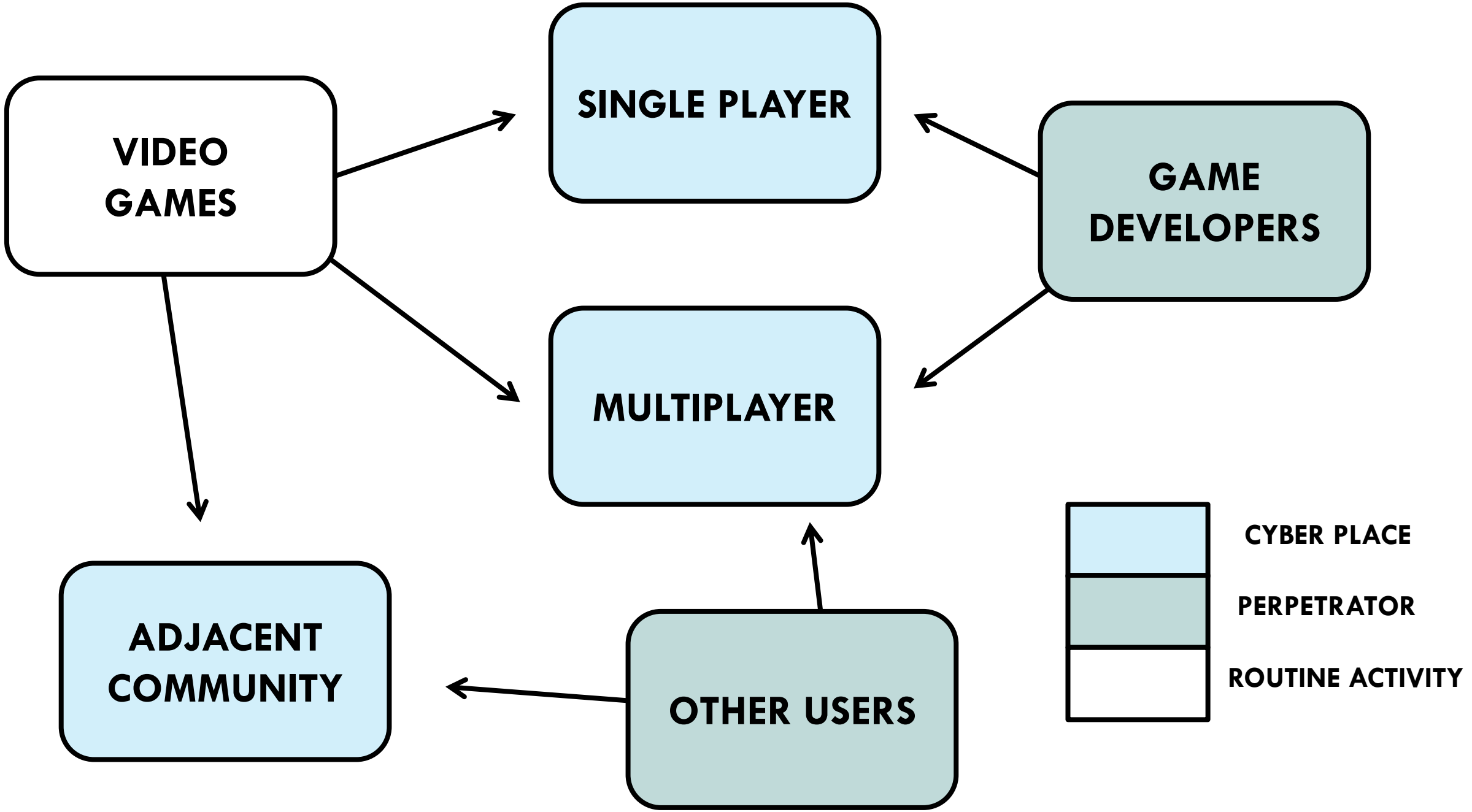
Adjayecent community:
User to developer and user to user interactions

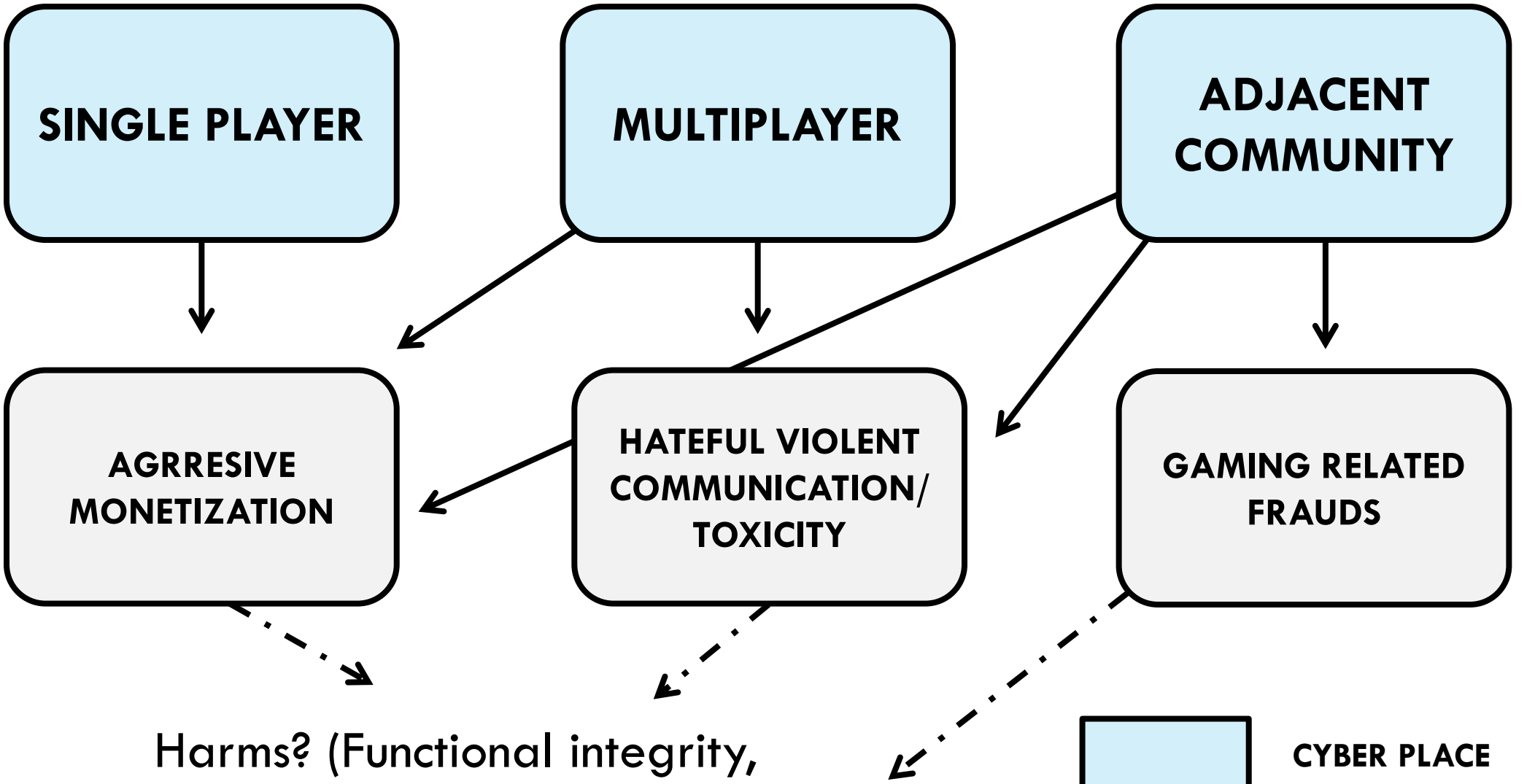
Resident Evil 4 by Capcom

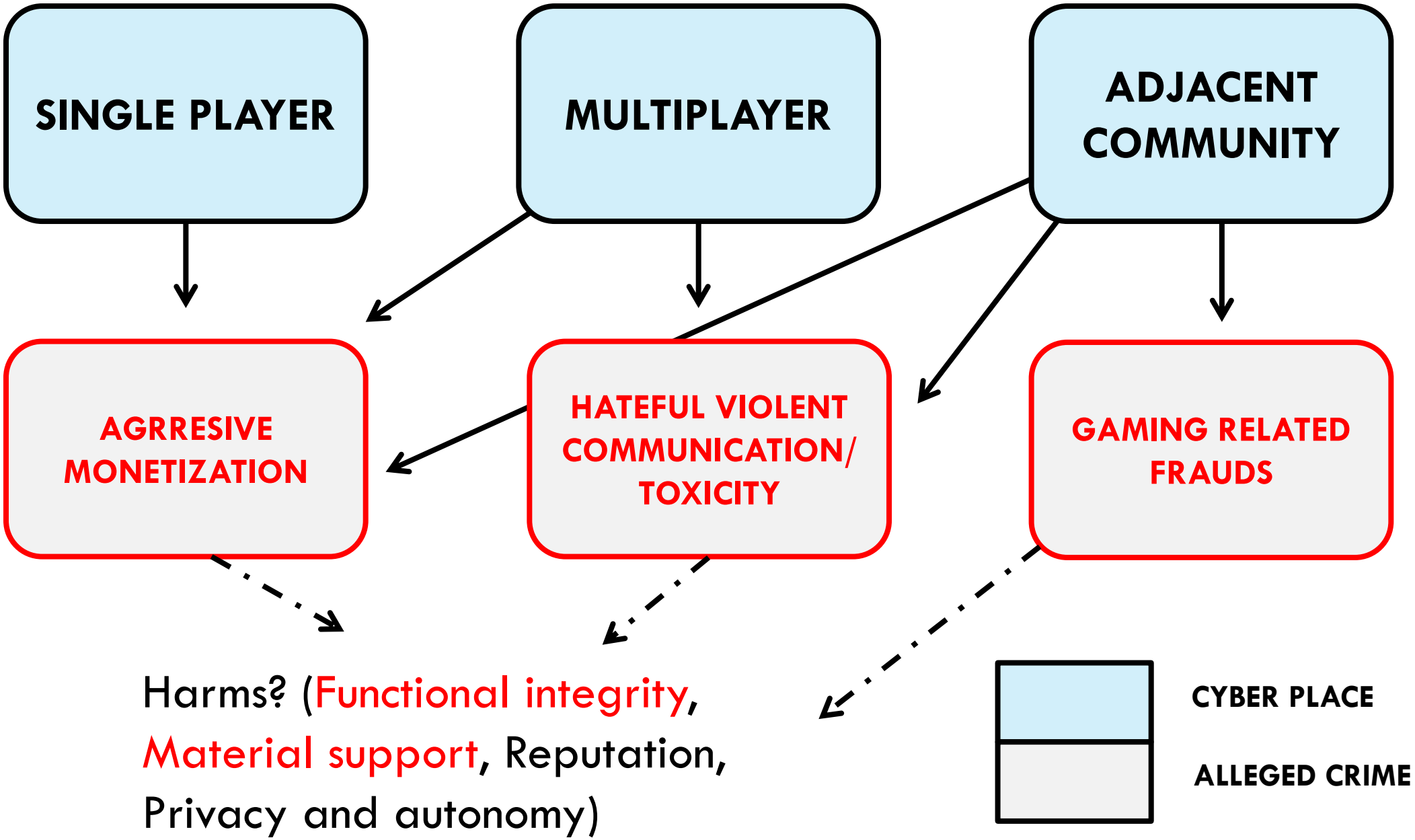
League of Legends by Riot

reddit

twitch


VIDEO GAMES
SINGLE PLAYER
GAME DEVELOPERS
MULTIPLAYER
ADJACENT COMMUNITY
OTHER USERS
CYBER PLACE
PERPETRATOR
ROUTINE ACTIVITY


SINGLE PLAYER
MULTIPLAYER
ADJACENT COMMUNITY
AGRRESIVE MONETIZATION
HATEFUL VIOLENT COMMUNICATION/ TOXICITY
GAMING RELATED FRAUDS
Harms? (Functional integrity, Material support, Reputation, Privacy and autonomy)
CYBER PLACE
ALLEGED CRIME


SINGLE PLAYER
MULTIPLAYER
ADJACENT COMMUNITY
AGRRESIVE MONETIZATION
HATEFUL VIOLENT COMMUNICATION/ TOXICITY
GAMING RELATED FRAUDS
Harms? (Functional integrity, Material support, Reputation, Privacy and autonomy)
CYBER PLACE
ALLEGED CRIME

AGRRESIVE MONETIZATION

Developer/user convergence: game developers exploit users' property by introducing aggressive monetization tactics that lead to the gamblication of those spaces: loot boxes as the most well-known example

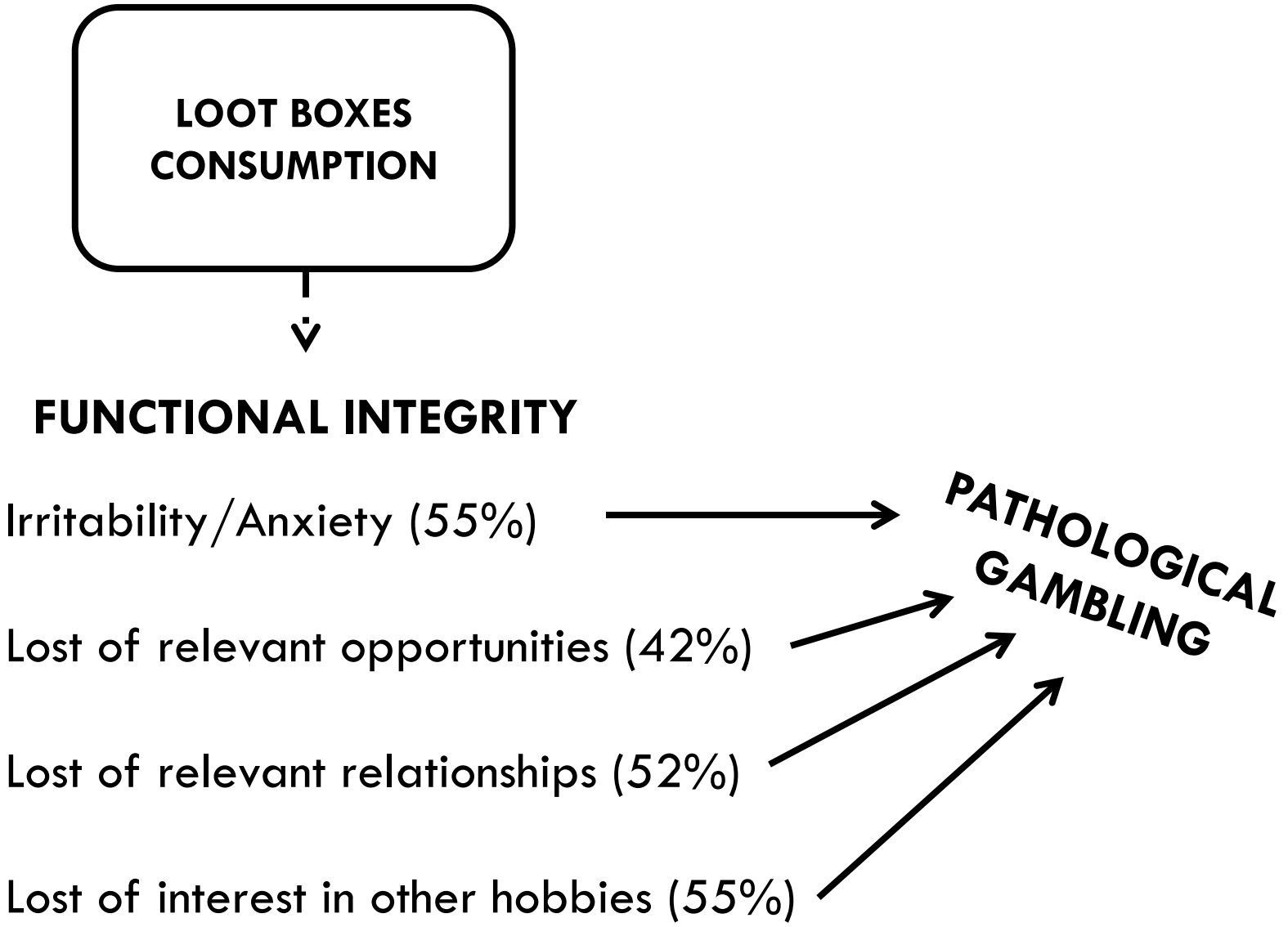
Prevalence in games: There is an habitual presence of monetisation and Lootboxes in video games, in games rated for under 18s (Aguerri y Tejada de García de Garayo, 2025).

Profile: The profile of players who participate in video game gambling is **predominantly young and male,** with a **high prevalence of students** (Coloma Carmona et al, 2024).

Criminalization or prohibition? The criminal policy question if this gambling mechanics shall be allowed in video games directed to children

Agressive monetization	n	Porcentaje
Investment in loot boxes	153	8%
Investment in in game assets	400	22%
Investment in game performance boosters	286	16%

SOURCE: GamerVictim proyect victimization survey to a sample of 1812 video game players



SOURCE: GamerVictim proyect victimization survey to a sample of 1812 video game players

GAMING RELATED FRAUDS

Lose of accounts: players engage in trade of accounts, losing digital assets (skins, game progress) (Kristiansen and Vassard Jensen, 2023)

Gaming consumer fraud: players buy digital products that are no returned (keys of digital games)

Influencer and investment fraud: the image of influencers and or celebrities is use with or without their consent to promote investment in cryptocurrency and trading frauds

Gaming related fraud	n	Porcentaje
Investment fraud	153	8%
Consumer fraud	188	10%
Investment in scam courses	164	9%
Theft of account	298	16%

SOURCE: GamerVictim proyect victimization survey to a sample of 1812 video game players

FUNCTIONAL INTEGRITY

Deterioration of habits (43%)
Physical symptoms (Stress/Nervousness) (35%)
Sadness (36%)
Suicidal thoughts (23%)
Shame/Guilt (43%)

MATERIAL SUPPORT

Reduced consumption game (45%)
Game Abandonment (41%)
Loss of interest/enjoyment (42%)

SOURCE: GamerVictim proyect victimization survey to a sample of 1812 video game players

THE PROBLEM OF… TOXICITY?

A research on "toxicity": An interest of game developers, players and academia on tackling toxicity or disruption

Prevalence of behaviours: social or political cybercrimes on some video games (Aguerri et al, 2023) and maybe in some video game genres (Zclila et al, 2022)

The harm principle and toxicity: the harms helps us to conceptualise and give priorities regarding criminal policy response

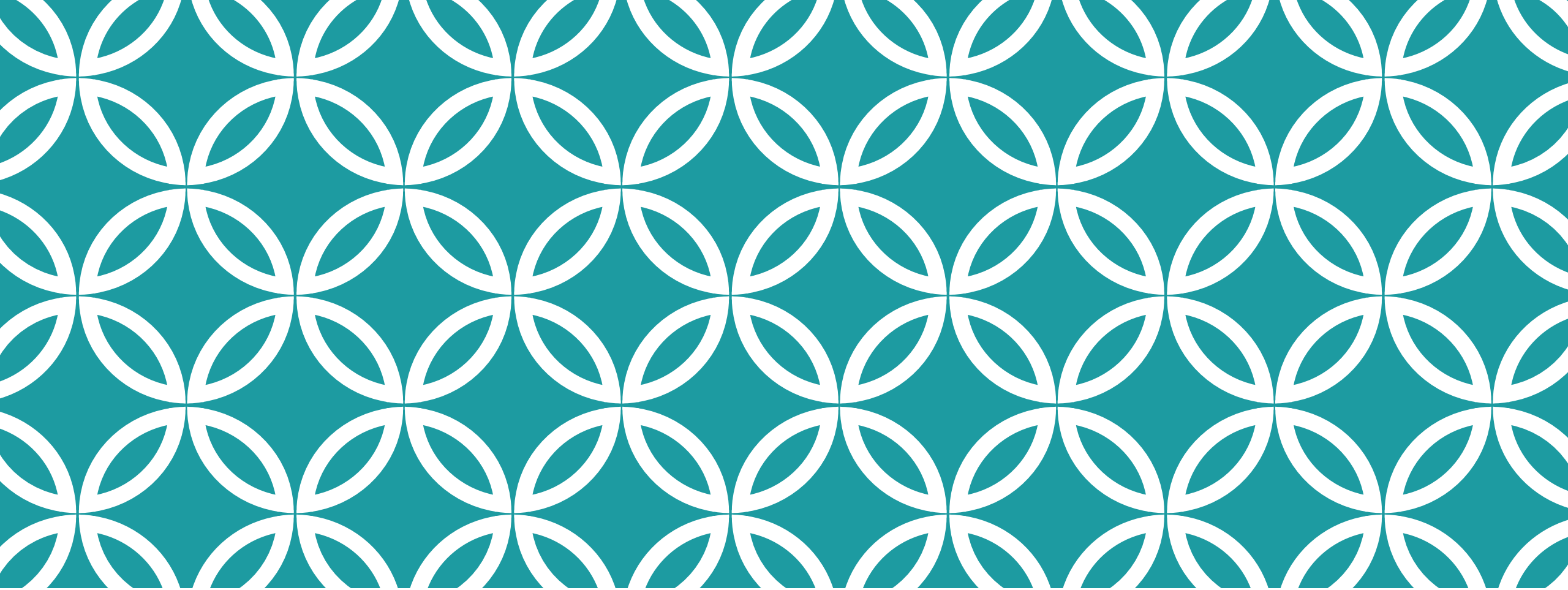
Behaviour	n	Percentage
Offense race	161	9%
Offense gender	142	8%
Offense general	216	12%
Fake complaint	164	9%
Cheating	191	11%
Critic of gameplay	212	12%
Sabotage of game	197	11%

FUNCTIONAL INTEGRITY

Deterioration of habits: disruption (50%) offence (59%)
Physical symptoms: disruption (25%) offence (39%)
Sadness: disruption (32%) offence (50%)
Suicidal thoughts: disruption (17%) offence (28%)
Shame/Guilt: disruption (25%) offence (38%)

MATERIAL SUPPORT

Reduced consumption game: disruption (51%) offence (60%)
Game Abandonment: disruption (50%) offence (54%)
Loss of interest/enjoyment: disruption (46%) offence (58%)



3. ARTIFICIAL INTELLIGENCE AND HARM

reface

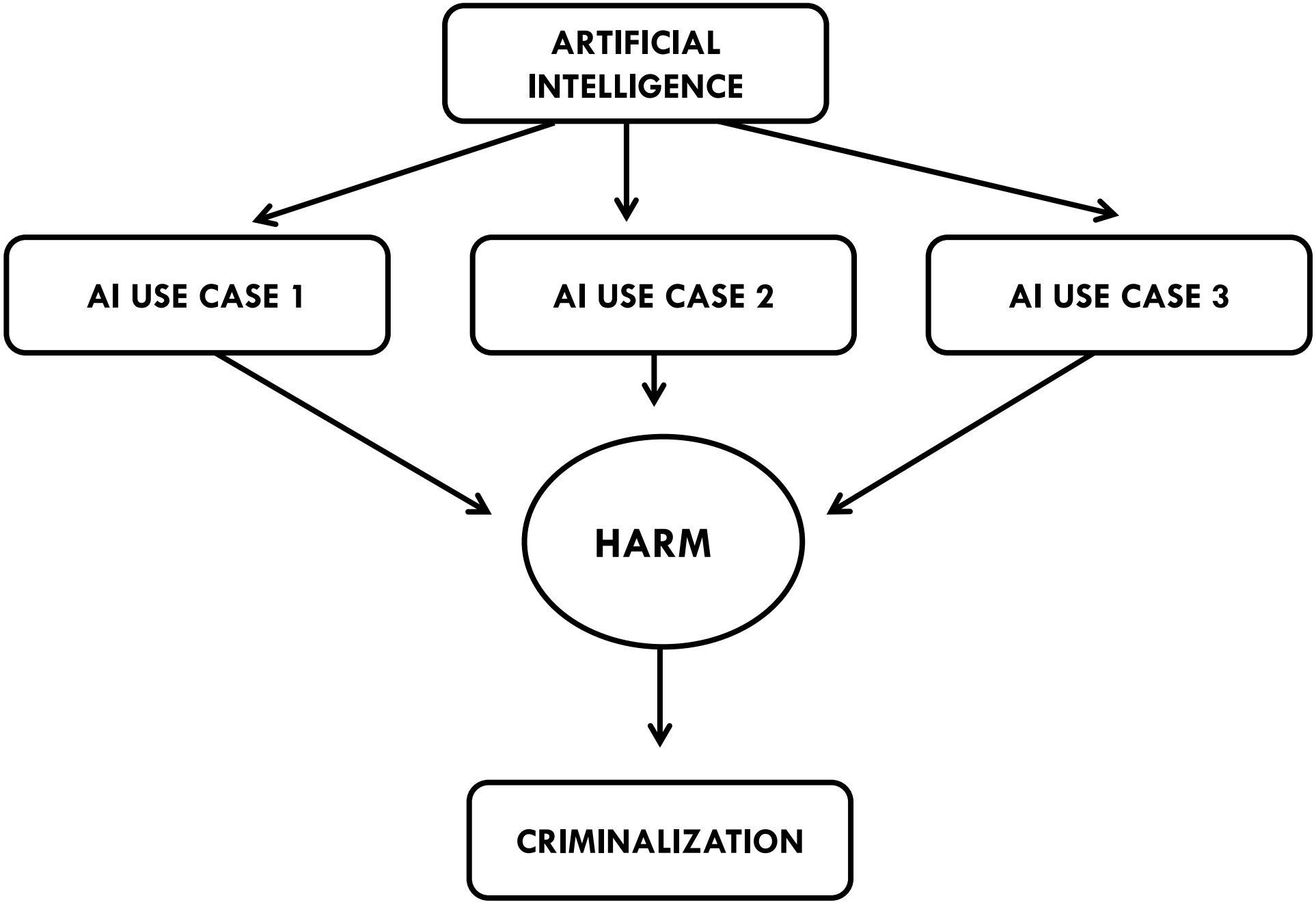
Reface AI: The Game-Changer in Content Creation

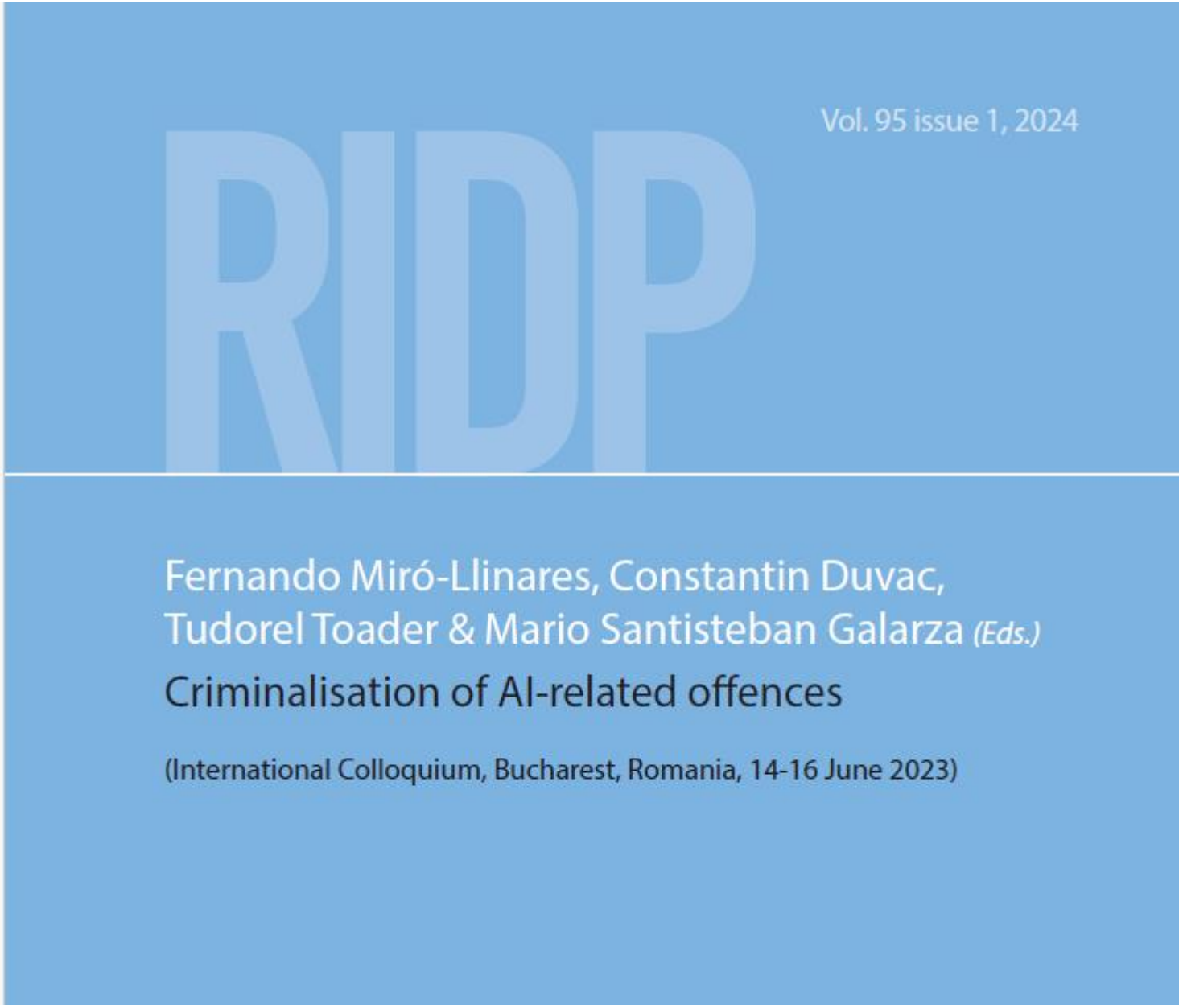
App to craft Deep fakes

OpenAI

Sam Altman, CEO Open AI (ChatGPT, DallE)

¿ Do we have to modify the Penal Code to punish behaviour due to the potential harmfulness of a developing technology and we don't know what damage it can cause?


ARTIFICIAL INTELLIGENCE
AI USE CASE 1
AI USE CASE 2
AI USE CASE 3
HARM
CRIMINALIZATION



A cross-analysis of 22 national reports and 4 special reports. Most of the reports come from countries in continental Europe (Spain, France, Italy, Austria, the Netherlands, Belgium, Greece, the Czech Republic and Germany) and Eastern Europe (Poland, Hungary, Croatia, Russia, Turkey, Ukraine and Romania), but there are also reports from Latin America (Argentina, Chile and Peru), Africa (Egypt), Northern Europe (Finland) and Asia (China).

Case 1. In China, criminals used AI to create programmes that dialled several telephone numbers with very realistic automated voices, scamming more than 300 people and obtaining more than 3 million CNY.

Case 2. In China, deepfake technology was used to impersonate a colleague and defraud a victim of 3,000 CNY.

Case 3. In China, a deepfake of a victim's boss's voice was used to request a transfer of 20,000 CNY.

Case 4. In Germany, the use of deepfakes to imitate the voice of a senior executive in a corporate fraud case was reported.

Case 5. In Ukraine, the use of a Telegram bot to facilitate the automated sale of drugs, providing buyers with information on locations and payment methods, was reported.

Case 6. In Germany, a deepfake of Chancellor Olaf Scholz was created for political manipulation.
Case 7. In Italy, Giorgia Meloni claims to have been the victim of a pornographic deepfake.
Case 8. In Turkey, a deepfake sex video was used to blackmail a businessman.
Case 9. In Spain, deepfakes of minors were used to create nude images of their classmates.
Case 10. In Turkey, a criminal created an Instagram account with pornographic content using a student's profile photo and deepfakes to replace her face in obscene images.

Case 11. In Italy, a programme collected personal data from telephone numbers obtained illegally to be sold in advertising campaigns, as part of 'Operation Data Room'.

Case 12. In Austria, a traffic accident involving injuries was reported, caused by an intelligent vehicle.

Case 13. In China, two accidents involving autonomous vehicles in 2016 and 2021 resulted in the death of the drivers.

Case 14. In France, an accident involving an autonomous vehicle in Paris was reported, causing material damage.

Case 15. In Finland, an accident involving a Tesla in autopilot mode resulted in the driver being convicted of creating a traffic hazard.

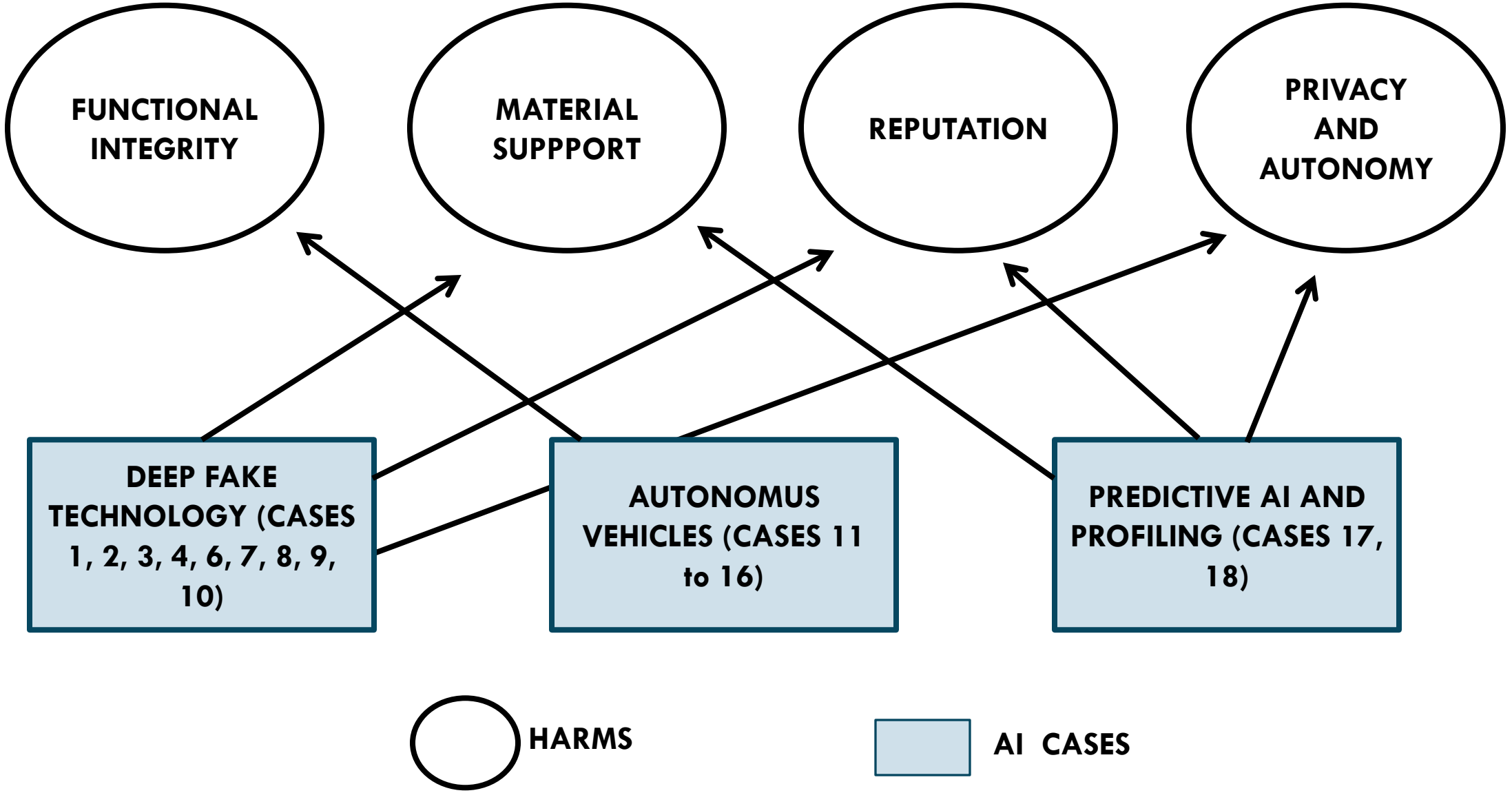
Case 16. In Arizona, USA, an autonomous Uber vehicle killed a pedestrian, and the driver was convicted of negligent homicide.

Case 17. In the Netherlands, an algorithm was detected that discriminated in the allocation of benefits to parents, affecting 26,000 families.

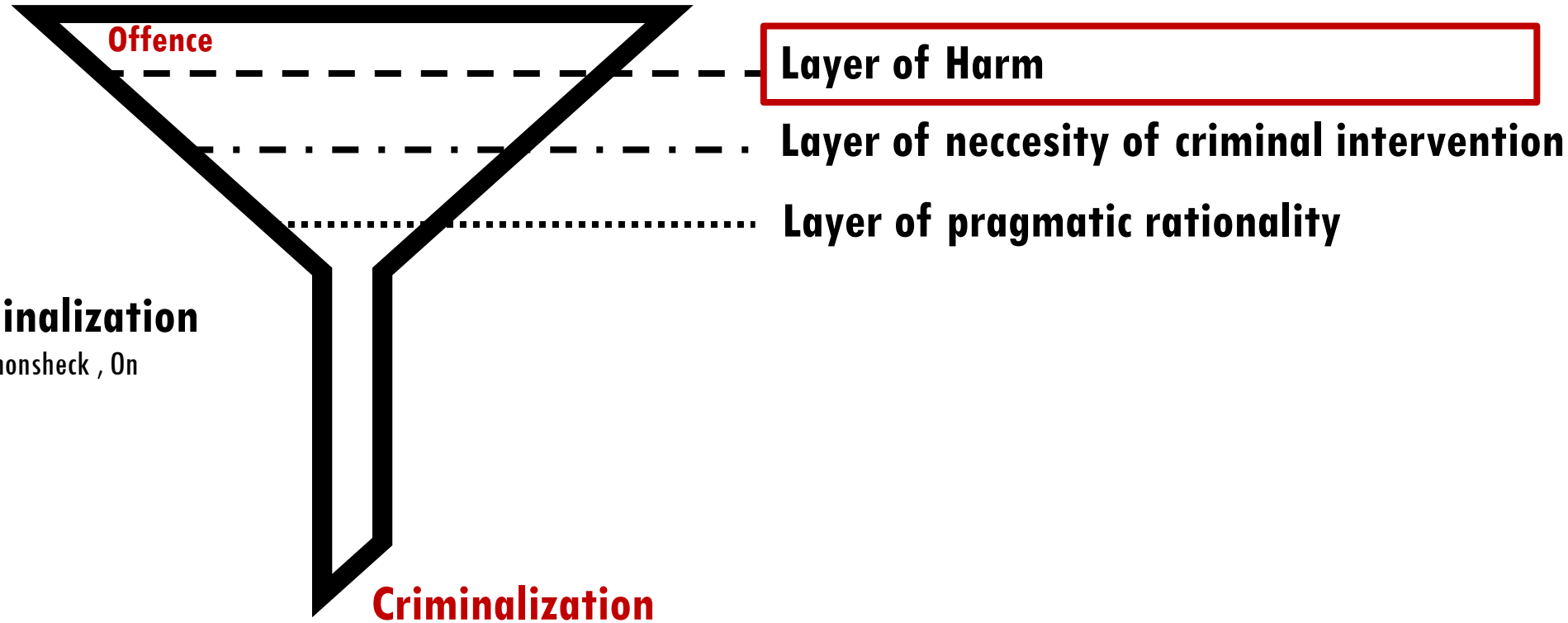
Case 18. In Italy, an algorithmic tool was implemented that generated reputation scores without the user's consent.

Case 19. In South Korea, a flaw in ChatChatGPT allowed users to see brief descriptions of other users' conversations and payment details.

Case 20. In China, AI was used to develop songs that imitated the structure of copyrighted works.


FUNCTIONAL INTEGRITY
MATERIAL SUPPPORT
REPUTATION
PRIVACY AND AUTONOMY
DEEP FAKE TECHNOLOGY (CASES 1, 2, 3, 4, 6, 7, 8, 9, 10)
AUTONOMUS VEHICLES (CASES 11 to 16)
PREDICTIVE AI AND PROFILING (CASES 17, 18)
HARMS
AI CASES

IS HARM THE ONLY RELEVANT PRINCIPLE? A PROCEDIMENTAL MODEL OF CRIMINALIZATION



Layers/filters of criminalization

(Miró Llinares 2023, adapted from Schonsheck , On Criminalization, 1994)

¡THANKS!

Fernando Miró Llinares

f.miro@crimina.es
@FernandoQPH