Public Governance, Administration and Finances Law Review

LUDOVIKA
UNIVERSITY PRESS

1.
2024

Public Governance, Administration and Finances Law Review

Vol. 9. No. 1. 2024

LUDOVIKA
UNIVERSITY PRESS

Contents

This page intentionally left blank.

Government Cybersurveillance and AI: A New Equation[1]

Michael Losavio*

* Associate Professor, Department of Criminal Justice and Department of Computer Science and Engineering, University of Louisville, Louisville, Kentucky, USA, e-mail: mmlosa01@louisville.edu

Abstract: There is a tension between state oversight and state intrusion into our personal lives. The analytical powers of artificial intelligence/machine learning and the pervasive data collection of the Internet of Things, the Smart City and all those personal devices we use together permit revelations as to our lives as never seen before. We must consider the impact of this on the relations between citizen and government in this new, ubiquitous world of government cybersurveillance and revelation.

Keywords: surveillance, cybersurveillance, artificial intelligence, algorithms

1. Technology and privacy

There is comfort, as children, in being watched over by family and friends as we play, do homework, sleep. That sometimes changes as we grow older. For some being surveilled by a parent, or the state, becomes a gross intrusion into our privacy and personal autonomy. The concept itself comes from the French "sur", meaning "over" and "veiller", meaning "to watch". For others, being watched over remains a blanket of safety in a world of evolving threats. Those relationships between citizen and state now evolve in a data world of constant surveillance. Information for that may come from data generated by the Internet of Things to Smart City administrative systems, from locational data of a cellphone to networks of closed-circuit television cameras. The huge, usually voluntary engagement with social media creates vast troves of information on peoples' lives. Much of that is open to public view, and easily accessible through a law enforcement request or search warrant where there is probable cause for a crime. It may also lead to concern and litigation of the impact of such systems on mental well-being. The San Mateo Board of Education is suing YouTube and other social media systems for

---

[1] This paper was first presented at the Forum on Privacy and Governmental Transparency (Ludovika University of Public Service) on 8 June 2023.

causing emotional and psychological injury to its minor students.[1] The impact of such massive surveillance may affect those relationships across all domains of society. Some see it as the future of policing and governmental public safety (Davidson, 2019). Others see it as a means to "predict enemies" (Deeks, 2018).

Jones v. United States[2] presented the United States Supreme Court with the question of the legality and propriety of inexpensive and easy computer mediated tracking via small devices placed on a suspect's automobile by law enforcement. The Court found such tracking invaded the privacy of the person tracked and would require a court order/search warrant upon a showing of probable cause of a crime, but decided the matter on traditional trespass grounds. Anticipating issues to come with government computer-mediated surveillance, Associate Justice Sonya Sotomayor opined in her concurring opinion that such extensive surveillance technology may very well come to change the relations between citizen and state.

The police powers of the state are as fundamental as they are intrusive, involving investigation, detention and punishment of people. As in many other areas of human activity, the role of computing – data collection and analysis – in policing has been growing. In particular, the use of systems for "predictive policing" use data to forecast areas of risk and, in some matters, individuals of risk who may be subject to special scrutiny and police attention. That additional scrutiny may become a self-fulfilling prophecy of guilt, even where there is none.

Computing has changed many aspects of our lives, especially our privacy, autonomy and safety. It changes the power of the government to see into the lives of its citizens in unprecedented ways. This has led to jurisprudence seeking to protect people in the face of new technology, just as where the question of privacy into the ruling in *Kyllo v. United States*[3] barring infrared surveillance of a home without a warrant, even where there was no physical intrusion to the home. The line of cases from *Jones v. United States, Riley v. California*[4] and *Carpenter v. United States*[5] have reinforced privacy rights against our use of new computing applications, and their use by law enforcement to generate unprecedented information on the lives of others in the exercise of the police power of the state. Legislative protections lag in the United States, especially when compared to those of the European Union and its General Data Protection Regulation (hereinafter: GDPR).[6]

There are similar concerns as to commercial surveillance and data security practices that may harm consumers through intrusions into their private lives.[7] Regulations may look at how commercial organizations may (1) collect, aggregate, protect, use, analyse and retain consumer data; and (2) transfer, share, sell, or otherwise monetise that data in ways

---

[1] *San Mateo County Board of Education and Nancy Magee, in her official capacity as San Mateo County Superintendent of Schools v. YouTube, LLC, Google LC, XXVI Holding Inc., Alphabet Inc., Snap Inc., TikTok Inc. and Bytedance Inc.*, United States District Court for the Northern District of California, Case No 3:23-cv-01108, pp. 1–107.

[2] *Jones v. United States,* 565 U.S. 400 (2012).

[3] *Kyllo v. United States,* 533 U.S. 27, 34 (2001).

[4] *Riley v. California,* 573 U.S. 373, 381 (2014).

[5] *Carpenter v. United States,* 138 S. Ct. 2206, 2221 (2018).

[6] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

[7] U.S. Fed. Trade Comm'n, Commercial Surveillance and Data Security Rulemaking, 16 CFR Part 464 Trade Regulation Rule on Commercial Surveillance and Data Security Rulemaking (Aug. 11, 2022).

that are unfair or deceptive; in an extreme example of private-state data collaboration the U.S. military purchased the entire satellite surveillance imagery of an active battlefield by a private company, preventing others from accessing it during the battle (Campbell, 2001).

In turn, private surveillance methods implicate ways in which government surveillance may use those private surveillance resources to look into the lives of people (Campbell, 2001). That may yet implicate the privacy principles of *Katz v. United States* that the Fourth Amendment, the primary statutory protection of citizens' privacy in the United States, protects *people,* not places.[8] The principles in *Katz* led to the rule in *Riley* that personal electronic device could not be searched absent a warrant, and then to *Carpenter* that historical cell site location information on a cellphone user's activity, though collected and held by a private third party, could not be accessed as to track that user absent a properly issued search warrant. While U.S. statutes protect communications in real-time and stored electronic communications for a period of time, there are few other protections from government surveillance in the new data age from federal legislation. Yet these can be instructive. Chapter 121 of the U.S. Criminal Code, 18 USC §2701, et seq., addresses stored wire and electronic communications and transactional records access. It outlines a framework for guide government access to such data and procedures to do so as to offer privacy protections to the people involved with such communications.

The potential data space that supports surveillance keeps growing, with increases in the sources of data and means to store it for access and use. These are paralleled by increasing growth in analytical power to pluck that data from "practical obscurity" and put it to surveillance use. Those analytic systems have grown in power – artificial intelligence, machine learning, neural networks – to the point that they can infer from that data aspects of and conclusions about peoples' lives that, in the past, would have been difficult or impracticable to obtain. These analytical systems for public security are used around the world, and their use is increasing.

One survey of police in the United States found that 88% of respondents used data tools for police purposes. (International Association of Chiefs of Police, 2011). Such data collection, transmission and analysis can engage and support police resources from the investigation of singular criminal activity to ways in which law enforcement engages with its community (Losavio & Losavio, 2014). These systems can promote quick, timely identification and apprehension of suspects, as well as mis-identify the innocent as offenders (CBS, 2013; Bensinger & Chang, 2013; Dyer, 2013; Connors & Zauderer, 2013). Recognition of these issues have led, in some cases, to law enforcement policies and training on the proper acquisition and use of such data, including open source social media and local sensing networks (Stuart, 2013).[9] It seems that fewer and fewer human activities can escape police oversight once a person steps out the door of their home, physically or virtually. The 2013 Rand Corporation study *Predictive Policing* examined the use of data analytics in public safety across the United States (Perry et al., 2013). Its observations showed a broad application of data analytics to a variety of public safety/crime issues.

---

8   *Katz v. United States*, 389 U.S. 347 (1967).
9   United States Department of Justice Global Justice Information Sharing Initiative Federal Advisory Committee, 2010. Online: https://shorturl.at/jwFNR

Some of these systems of police analytics were effective. Others, however, were less so, raising issues as to whether or not they should even be used.

With these new computing technologies, we are presented with five fact domains that may impact the intrusiveness of government surveillance. And how those intrusions may be mitigated if we wish or need to do so.

Five technical concerns should be considered in relation to new computing technologies and their use in government surveillance; those are:

1. What are the data at issue, and its data subject?
2. How and where are those data sensed, perceived and generated?
3. How, where and under what conditions are those data collected and stored?
4. How are such data accessed and analysed?
5. How are those data and analysis used?

These domains reflect constitutional, statutory and common law privacy issues under U.S. law, and similar characterisations under the General Data Privacy Regulation of the European Union and the proposed EU Artificial Intelligence Law.

Table 1 details how a technical node may risk compromise as to particular privacy and security interests:

Table 1.
Risk nodes mapped to privacy and security

Risk node	Privacy breach	Security breach
Sensors	Intrusion	Hijacked/spoofed instrumentation, or erroneous data
Networks	Transfer beyond control	Interception, masquerade, hostile injection
Analytics	Revelation, mis-inference	Mis-inference, false negatives, false positives

Source: Compiled by the author.

Such compromise may be matched to outcomes from that compromise as to direct where protections for personal privacy and security could be directed for the most effective protection of those interests from attack.

These reflect points at which regulation may be used to protect privacy and security from new areas of surveillance. Regulation as to conduct and the engineering of these systems may offer privacy protection in this computational age through limitations on the use of these technologies in adverse ways. A regulatory control may mandate technical and engineering protections, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule[10] on protection obligations, its Security Rule[11] on required controls for electronic personal health information and the GDPR restrictions on transfer of personal data across borders. Technical regulation can support privacy and personal autonomy, though the engineering must be flexible to permit regulatory audit and

---

[10] HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 (2000) (US). Online: https://t.ly/BJplX
[11] HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164 (US) (2010).

response; the HIPAA Security Rule requires entities under the jurisdiction of the Security Rule, such as health care providers and those they contract with that access personal health information (PHI) must:

- ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
- identify and protect against reasonably anticipated threats to the security or integrity of the information
- protect against reasonably anticipated, impermissible uses or disclosures
- ensure compliance by their workforce

The ways in which persons may be injured by the improper use of such information, including PHI, as to need regulation for protection is seen in Table 2 below. Table 2 details governance of technology and system use as to provide controls that, in turn, may protect against particular injuries to personal privacy and autonomy.

Table 2.
Governance of technical operations and use creating protections

Systems issues	Regulatory controls	Privacy injuries mitigated
Sensed and networked data	Use limitations and filters, controls over transmission	Improper publicity
Analytics against the networked and collected data	Data limits, bi-directional network limits, use limits	Intrusion into private affairs
Incomplete data, network gaps and flawed analytics	Assurance criteria for data, vetted algorithms	Mis-inference, false assertions, false light

Source: Losavio et al., 2018

Whether by the government or private parties, new systems of data-driven surveillance can change the dimensions of the space of personal autonomy, shrinking it more and more. It may indeed change the relationships between people, civil society and government where people no longer feel secure from their government nor from malicious private parties.

2. The data at issue, its data subject and the provenance of data for surveillance

Data about individuals are the primary issue and concern in state surveillance as it provides direct evidence of activities and inferences and conclusions about a person. These may range from where they were at a particular time or what they may have purchased that could be put to malicious purpose. This data can be compiled to create a profile on

a person as to impact the individual as a data subject and as to their person and professional life. That data may directly connect to a data subject or permit inferences about that data subject, to varying degrees of specificity and identification. Closed circuit video or an investigator's images of a person may connect directly to a specific person, correctly or in error. Credit card use, payment systems, cellphone use and automobile license plate readers provide a one-off inference that possessor/owner of the related technology is using it. All these data are subject to analysis by analytical engines of computation.

These data objects, depending on system design, may be accompanied by related metadata such as time, place, activities and associations of the data subject. As the amount of information expands, more direct and inferential conclusions may be made about an individual. Whether those conclusions are correct or not represent the particular risk in their use. This may lead to potentially significant damages to the person that is connected to those conclusions. A significant risk now comes from the reliability of artificial intelligence systems in assembling and analysing data; this risk may be heightened by the lack of transparency and the ability of those who build such systems to explain the operations of those AI systems. These factors can impact the measurement and detection of such risks as well as creating them.

Data are the starting point, the grist for the analytical mill. Artificial intelligence brings a renewed relevance to the old computational saying "Garbage In, Garbage Out". The provenance and quality of the data used to develop AI systems and used by them to produce results are vital concerns. They are critical for weighing the reliability of a system in making any conclusions at all, as required by judicial rules of evidence. In the world of semi-supervised and unsupervised machine learning, AI systems teach themselves through their analysis of large bodies of data, such as Large Language Models. Bad and corrupt data, and data based on improper, illegal or unfair rules can lead to the creation of badly corrupted algorithms. Those corrupted algorithms may then generate corrupt and erroneous conclusions about their data subjects. And the targets of a police investigation.

Even where AI systems are built on good data with algorithms that perform as programmed, problems may develop in how those systems are used absent ways to assure the reliability of the data output of the systems. This is vitally important and a growing challenge with the rise of "deep fake" technologies that make forensic determinations of authenticity more and more difficulty. Images, audio and video may all be subject to "deep fake" manipulation and fabrication, even as images, audio and video represent some of the most powerful evidence considered by a finder of fact such as the jury. Because of this new challenge to authenticity, it becomes vital to see and judge how data is created and collected, and possible solutions to the problems of provenance in a time of deep fakes.

3. How data is sensed, perceived and generated for surveillance

A starting point for validating provenance and reliability, if possible, is how data is generated and created. Where data is created by an electronic system there must be some evidence of the reliability of that evidence. The accuracy and reliability of the

sensing or perceiving system that generates that data is of primary importance. As that data may not be directly authenticated by a human observer who can testify that the data and representations are accurate and representative, other evidence of reliability will be needed.

System testing and evaluation such as required for the validation of expert evidence under rules like the Federal Rules Evidence 702 and 703 of the United States may establish the reliability of that data sensing and generation. For electronic and digital systems this may be particularly important as the complexity of the systems increases. For artificial intelligence systems this is particularly critical due to issues with the transparency and "explainability" as to how such systems operate and produce results and conclusions. These issues may be difficult to resolve as to assure reliability under rules for judicial resolution (Federal Rule of Evidence 702 US 1973; Federal Rule of Evidence 703 US 1973). Those rules provide controls on the admission of expert-proved evidence such that certain "tests" must be met for the use of such expert-proved evidence.

FRE Rule 702 provides that:

> Federal Rule Evidence 702 (US) A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue
> (b) the testimony is based on sufficient facts or data
> (c) the testimony is the product of reliable principles and methods; and
> (d) the expert has reliably applied the principles and methods to the facts of the case

FRE 703 provides that:

> An expert may base an opinion on facts or data in the case that the expert has been made aware of or personally observed. If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.

These requirements may be difficult to meet, especially for unsupervised or semi-supervised artificial intelligence and machine learning systems where, in part, the system is effectively programming itself to do certain tasks.

For electronic systems that have provided evidence in legal fora in the past, such as photographic and video cameras, some fora permit inferential validation by testimony that the system is regularly used, was used as it was meant to be used, and operated properly. The burden is shifted back onto those challenging the evidence to show that the system was not working properly and cannot be relied upon reliable evidence.

This may be difficult where the systems cannot be evaluated due to their complexity and occult operations. Testimony that the system has been in use and operates properly

may not be sufficient especially where digital imagery can be easily manipulated; deep fake systems are designed for difficult-to-detect manipulation. Such systems may not be available for evaluation and study as to aid in the detection of their use.

The growth in number and variety of sensing devices connected via Internet technologies greatly expands data generated on everyone and available for analysis. Validating the reliability of this data collected becomes even more important. An inventory of the ways in which data can be sensed and transmitted to central storage and for analysis demonstrates the broad and ubiquitous means by which human activity can be surveilled. A partial inventory includes these sensing systems, whether individual or as part of larger data collection systems and shows the plethora of devices for capturing aspects of the lives of others:

- video surveillance and identification
- video surveillance and behavioural inference
- audio surveillance (ShotSpotter for neighbourhood gunfire)
- license plate readers
- automobile networks and toll scans
- Smart City technology
- Cell Site Location Information (CSLI)
- other sensor networks
- RFID
- home IOT devices
- out of home IOT devices
- other sensors that come with evolving technology

Each of these systems generates information of varying types, all accompanied by various types of metadata, such as time and place, which allow additional inferences regarding a data subject's activities. Video information can be fed into facial recognition systems that, along with the time and location data of the video, can place a person in a particular place at a particular time. Cell site location information (CSLI) can place an individual proximate to illegal or embarrassing activity, with varying degrees of accuracy and precision.

Law enforcement agencies have sought CSLI information that might connect individuals in a state that prohibits pregnancy termination to pregnancy termination clinics in another state. Audio surveillance for gunshots as to time and location can direct of additional police resources to a particular location; those police resources have been informed of possible "shots fired" and may respond accordingly, with guns drawn. Data analytics against image technology can "identify" suspects and possible offenders, but an error rate in the analytics may lead to erroneous mortal outcomes for predictive policing.

License plate readers, service tagging devices such as for toll roads, and "Smart Cities" implementations of sensing devices can support services ranging from traffic management to public health. They provide a skein of data for both directly managing related services. But such data profiles can be used, alone or in conjunction with cross matching against other data, to create profiles on individuals or classes of individuals. The growth of the Internet of Things and all of the sensing and data collection devices associated with such

systems, within homes, within businesses and in the public world, create another bounty and wealth of data that can be accessed and collected for analysis.

Where that information is proximate to potential illegal activities, it may create the foundation for further state surveillance and investigation of an individual, regardless of the guilt or innocence of that individual. It also creates the ability to profile and make inferences on the lives of individuals in unprecedented ways. This may or may not be within the purview of the state but, nonetheless, puts immense power in the hands of state actors to use. Such uses may not be in the interest of the individual but that of others seeking to manipulate and impact her.

The domains of different nodes for the creation and transmission of data present offer guidance for regulation and engineering to preserve privacy. Regulation may involve some or all of these information spaces as to protect privacy, as shown in Figure 1.
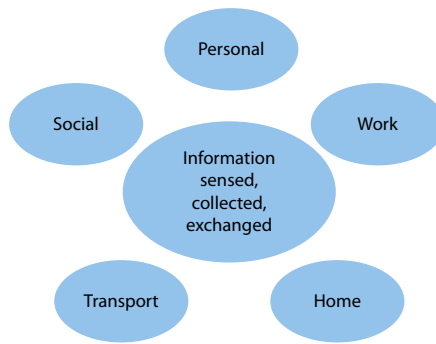
Figure 1.
Data nodes of activities and services

Source: Losavio et al., 2018

4. How data is collected and stored for surveillance

After the sensing and generation of data, it is available for use. While that use may be local at the sensing device, there is greater utility in the collection of large amounts of data for more sophisticated analysis and broader use. The Internet of Things paradigm extends from the local generation of data to its transmission and collection, often through Internet technologies. After transmission there is the collection of the data various points for use. The evolving topology of the Internet of Things now includes Edge computing, Fog computing and Cloud computing. In Edge computing data is collected close to the point of generation for use and analysis, either locally or for downstream transmission. Fog computing are those systems connected in the space between the Edge/sensors and the Cloud computing environment; Fog computing allows for regional aggregation and analysis of data and use. The Cloud metaphor for computing addresses endpoint services of massive storage and computational power connected globally to provide services and data processing results as needed.

Whether through Internet systems or through private networks, regulation may be applied within the various space of the topology. The GDPR limits data transmission across national boundaries, defining the facts that indicate relevant regulation of data transmission, analysis and usage within that apology can be controlled.

The topology, or structure by which data is collected, transmitted and stored encompasses a wide variety of systems. The systems may be mobile or stationary, domestic transnational, proprietary/third party, governmental or open source. All of these areas may be subject to regulation, including controller transmission and exchange of data.

Limits on government access to data, including third party data can have similar protective benefits through those limitations. Such protective regulation includes these as to reinstate the "practical obscurity" that allowed privacy over time, similar to the "right to be forgotten".[12] An expansion of the notion of "practical obscurity" would likely provide for redaction of the information in records as a means of protection for privacy. But the ability of electronic databases to tag particular data as to obscure it from certain search requests, especially those from a particular jurisdiction, may let such delisting be sufficient subject to damages where it fails to conceal that information.

Examples of such protective limits and practices may include:

- government limits on data exchange
- First Amendment (U.S.) freedom of speech limits on regulation of data exchange
- GDPR limits on data exchange
- voluntary limits on data exchange
- personal responsibility for data generation, data transmission data exchange

Similarly, protections are seen in Article 17 of the GDPR:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
    c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
    d) the personal data have been unlawfully processed;
    e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
    f) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as

---

[12] *United States Department of Justice v. Reporters Committee for Freedom of Press*, 489 U.S. 749 (1989).

the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

g) for the establishment, exercise or defence of legal claims.

The means to meet compliance with these rules by search engines was detailed in *GC and Others* EU:C:2019:773.[13] The jurisdictional scope of such rules was set out in *Google v. CNIL* EU:C:2019:772.[14]

Personal responsibility for data generation, data transmission and data exchange offer another means of protection. An individual's care in maintaining privacy may preserve that privacy, but only if attention is paid to efforts to obtain a person's agreement to surrender that privacy. All manner of contracts contain specifications for the release of private data. A person – a data subject – may "opt out" of such disclosures, but often that requires a positive act, even if only checking a box, to invoke that protection.

5. How is that data accessed, analysed and used for surveillance?

The endpoint of data creation, transmission and collection is its use. The growth of powerful analytics, especially that denoted "Artificial Intelligence (AI)", make for new concerns about the power of government surveillance. The "practical obscurity" of individual data in large data collections is no longer possible given the power of analytics to sift through trillions of bytes of data quickly and, by analysis, both find otherwise obscure bits of information but also process that information to find patterns and relationships. That analysis can produce conclusions and inferences that would otherwise have been impossible in the past without the allocation of immense resources.

These powers of analytics represent new and dangerous possibilities for the use and misuse of the systems for government surveillance. Examples of the immense analytical power now available include generative AI and Computer Vision/Facial Recognition. These offer exceptional power for government surveillance to promote public safety. The GDPR data processing regulations offer some control over the ways in which these systems apply, although some worry it is not a sufficient control over such systems (Mitrou, 2018).

The European Parliament adopted the EU Artificial Intelligence Act to provide a broad regulatory framework for AI. That AI Act banned some AI applications, albeit with specifically delineated exceptions for law enforcement, and strict regulation of "high-risk systems". The co-rapporteur for the Internal Market Committee noted:

> We finally have the world's first binding law on artificial intelligence, to reduce risks, create opportunities, combat discrimination, and bring transparency. Thanks to Parliament, unacceptable AI practices will be banned in Europe and the rights of workers and citizens will be

---

[13] Case C-136/17 *GC and Others* EU:C:2019:773. See the text of the decision at https://doi.org/10.1093/grurint/ikaa003. *GC* outlines how search engines implement the right to be forgotten in their databases.

[14] Case C-507/17 *Google v. CNIL* EU:C:2019:772. See the text of the decision at https://doi.org/10.1093/grurint/ikaa004. CNIL sets out the territorial coverage of the right to be forgotten as to define the obligations of data holders to implement that.

protected. The AI Office will now be set up to support companies to start complying with the rules before they enter into force. We ensured that human beings and European values are at the very centre of AI's development.

Such restrictions as set out in the EU AI Act will limit how data and AI are used, albeit, with greater leeway for law enforcement pursuing public safety via such systems.

For the United States there is yet little regulation to date beyond common law principles and statutes relating to personal injury in violations of civil rights. A U.S. Artificial Intelligence regulatory statute is pending in the U.S. Congress. Other nations, such as the People's Republic of China and the Federative Republic of Brazil, have implemented initial regulatory statutes while pursuing further legislation. The United Kingdom has set out its own framework from which to begin its process of AI regulation.

This rush to build regulatory structures parallels the rapid growth in benefits and dangers from such systems. The concerns regarding AI mediated facial recognition systems for government surveillance derived from concerns as to reliability of the analysis and its subsequent use. Errors, whether false positives or false negatives, undermine the reliability of these systems, particularly as to gender and ethnicity where individuals from related groups may not have been adequately represented in the data training set (Axon, 2019). False negatives lead to a possibly guilty person escaping; false positives lead to an innocent person becoming the focus of police powers.

Regulation in this exceptionally important area of AI-mediated government surveillance can be problematic given the early stages of these technologies, particularly as to undeveloped standards for testing and validating these systems. It is a problem of not knowing what we don't know. This reflects some of the underlying problems in AI generally. The risks of injury from these problems and defects is especially high in government surveillance systems.

To assure the best outcomes from the use of Artificial Intelligence systems, those systems must be:
- transparent, in that their operations may be open to inspection and review
- explainable, in that the designers and operators of these systems understand those operations and can explain how the system produces the results it produces and the reliability that can be placed on those results
- accountable, in that where there is injury that results from these systems the responsibility for them can be allocated

Yet these may be elusive for a variety of reasons.

AI transparency may be hindered by the sheer complexity of those systems, especially where unsupervised self-learning algorithms have devised the operations beyond human coding. Those AI systems may also be hindered by efforts to protect proprietary design within the system.

AI "explainability" as to how an AI system operates is made difficult by the different ways in which the system may operate, especially where that system is trained to teach itself against large databases of information. Unsupervised machine learning algorithms are trained against large databases of information and code themselves to develop

result-producing algorithms from their analysis of that data. The resulted algorithms may not be human-mediated and may require extensive back analysis to understand their operations. Without that there may be no way to explain exactly what the system does; all that can be seen are the results of system operation. Waiting to evaluate those results after operation may lead to injuries of others as that evaluation is done.

AI accountability for damage done by AI mediated systems is itself hindered by the problems with the lack of transparency in operations and that the systems and their operations cannot be explained due to the way in which these systems developed. This makes the attribution of causation, whether to the developers/programmers, vendors or users, much more problematic. Further limitations on accountability may be found within the end-user license agreements that may accompany the transfer of ownership or license of an AI system to the user or third party.

6. The human-in-the-loop factor for surveillance: Additional protection or additional abuse

A factor increasingly seen as vital in the use of AI, and of particular importance when used for government surveillance, is the notion of the "human-in-the-loop" factor, that there is a human-mediating element to the use of AI systems. AI results should be subject to human review of the outcomes as to provide a critical limitation on damage from erroneous outputs. But the reliability of this component may vary, depending on the very competence or integrity of the particular human receiving a particular AI output in the surveillance of a person, community or nation. The human-in-the-loop aspect of AI systems for government surveillance raises additional concerns beyond making the system more reliable. The very integrity of that human becomes an issue as to proper vetting of the AI results as to rely on them.

The ethics review board of the Axon law enforcement technology vendor was charged to evaluate facial recognition technology and its utility for public safety. It specifically noted a problem where such system could be modified by system users; the risks of such manipulation within law enforcement were deemed further reason facial recognition technologies should not yet be deployed. But human engagement can have an impact on implementation of AI outputs; the State of Michigan's "robo-judge" system for determining unemployment insurance fraud went from a 90+% false positive rate to a 50+/−% false positive rate once human reviewers were inserted into the process.[15] Encouraging, but not sufficient. In the evaluation of LASER and PREDPOL analytical policing systems, the evaluators found errors relating to the lack of consistency in the human component as to data collection, analysis and implementation.[16]

---

[15] *Cahoo, et al. v. SAS Analytics Inc., et al.* ___ F.3d ___ (6th Cir. 2019) (US).
[16] Report of the Inspector General-LAPD, *Review of Selected Los Angeles Police Department Data-Driven Policing Strategies,* March, 2019.

One indication of the importance of the human-in-the-loop is the notion of "prompt engineering" in support of the use of Large Language Models (LLM) (Saravia, 2022). These LLMs are essential to the training of GPT systems.

This is the idea that most effective use of generative AI and Large Language Models (LLM) such as ChatGPT is where the human can devise the most effective and efficient inputs to the system as well as be able to judge the reliability of the outputs. This will require a deeper understanding by humans of system operations and linguistic concepts as to build effective AI prompts. This is a nascent area of skill and ability that must be developed to provide better assurance of reliable outcomes.

Human engagement and attention to these operations can support reliability and accountability. It may be the final bulwark protecting subjects of AI analysis. But that assumes the competency of the humans involved. And their integrity and honesty.

The final implementation for reliability and safety in AI-mediated government surveillance will be assuring competency and integrity of the human component. That may require:

- testing and certification of human operator as to competency and integrity
- training of human operators to ensure competency and integrity of use
- a compliance regime to guide and assure proper use of AI systems that includes logging of operations and auditing of compliance by all elements in the system

Without this it will be much more difficult to know until *after* injury happens that the system was used improperly.

7. Conclusion – Balancing order v. liberty

These issues relating to AI reliability go beyond government surveillance and predictive policing into all implementations of these systems and the risks they pose (Gianni et al., 2022). This has led to nations seeking strategic approaches to the implementation of AI in public administration as to mitigate those risks (Dutton, 2018; Berryhill et al., 2019; Misuraca & Van Noordt, 2020). The EU Artificial Intelligence Act is an important first step in building a coherent regulatory framework that both promotes the amazing abilities of this technology and the protection of the rights of people who may be threatened by it.

Assuring proper use of AI-mediated government surveillance includes technical, legal and end-user issues that are part of AI governance. From design to implementation to compliance review, these are systems within which well-drafted mandates best assure the reliability and propriety of the systems and their use. Failure to create an effective system of governance that holds everyone to account in the chain of operations – from data to AI to human – destroys accountability and any incentive for fair and just systems.

How the state engages in this process of regulation is critical. There must be government control and government restraint and ethical use as to implementation, compliance and governance (Winfield & Jirotka, 2018). Such engagement may need to be more responsive and timely given the rapid change in the technology (Wallach & Marchant, 2018).

The broad use of the Internet of Things, such as RFID chips to tag so many things and the ability of CSLI to turn any cellphone in a tracking device, and the potential for their misuse, demonstrate the risks of ever-novel technologies.

This governance must be informed, intelligent and flexible. The uproar over AI systems, particularly generative pre-trained transformer systems like ChatGPT, makes this an immediate concern. There have been calls to freeze research and development on AI systems, a solution that will not satisfy nor protect anyone. Rather, this gives an advantage to research in regimes that have less scruples about these matters and may give them a competitive advantage in crucial areas. These include areas of public safety and national security, as the use of AI systems in cyberattacks is an increasingly sophisticated and cost-effective means to break down, infiltrate and exploit the cyber systems vital to contemporary life.

The engagement of public safety, law and AI specialists can promote this. Review and policy boards on AI are increasingly used to provide flexible and informed governance while promoting innovation. The failure to work together may lead to the terrible outcomes we fear. We must not let that happen.

References

Axon Enterprise, Inc. (2019). *First Report of the Axon AI & Policing Technology Ethics Board.* Online: https://shorturl.at/kyEHR

Bensinger, K. & Chang, A. (2013, April 20). Boston Bombings: Social Media Spirals out of Control. Los Angeles Times. Online: https://shorturl.at/nstEU

Berryhill, J., Heang, K. K., Clogher, R. & McBride, K. (2019). Hello, World: Artificial Intelligence and Its Use in the Public Sector. *OECD Working Papers on Public Governance,* (36). Online: https://doi.org/10.1787/726fd39d-en

Campbell, D. (2001, October 17). US Buys Up All Satellite War Images. *Manchester Guardian.*

CBS News (2013, April 24). Social Media and the Search for the Boston Bombing Suspects. *CBS News.* Online: https://shorturl.at/gJQTU

Connors, B. & Zauderer, A. (2013, January 2). Police Use Facebook to ID Waterford Robbery Suspects. *NBC Connecticut.* Online: https://shorturl.at/hmW34

Davidson, R. (2019, August 8). Automated Threat Detection and the Future of Policing. *FBI Law Enforcement Bulletin.* Online: https://shorturl.at/erPZ2

Deeks, A. S. (2018). Predicting Enemies. *Virginia Law Review, 104*(8), 1529–1592. Online: https://shorturl.at/lxyDM

Dutton, T. (2018, December 6). Building an AI World: Report on National and Regional Strategies. *CIFAR.* Online: https://shorturl.at/dlFJ3

Dyer, J. (2013, April 27). Social Media and the Boston Bombings. *BBC Radio.* Online: https://shorturl.at/gmoC0

Gianni, R., Lehtinen, S. & Nieminen, M. (2022). Governance of Responsible AI: From Ethical Guidelines to Cooperative Policies. *Frontiers in Computer Science,* 4. Online: https://doi.org/10.3389/fcomp.2022.873437

International Association of Chiefs of Police (2011). *Survey of Law Enforcement's Use of Social Media Tools.*

Losavio, J. D. & Losavio, M. M. (2014). Prosecution and Social Media. In C. D. Marcum & G. E. Higgins (Eds.), *Social Networking as a Criminal Enterprise* (pp. 197–220). Taylor & Francis. Online: https://shorturl.at/tBF69

Losavio, M., Elmaghraby, A. & Losavio, A. (2018). Ubiquitous Networks, Ubiquitous Sensors: Issues of Security, Reliability and Privacy in the Internet of Things. In N. Boudriga, M. S. Alouini, S. Rekhis, E. Sabir & S. Pollin (Eds.), *Ubiquitous Networking. UNet 2018.* Lecture Notes in Computer Science (LNCS), 11277. Springer. Online: https://doi.org/10.1007/978-3-030-02849-7_30

Misuraca, G. & Van Noordt, C. (2020). *AI Watch. Artificial Intelligence in Public Services.* Publications Office of the European Union. Online: https://doi.org/10.2760/039619

Mitrou, L. (2018). *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* Online: https://dx.doi.org/10.2139/ssrn.3386914

Perry, W. L., McInnis, B., Price, C. C., Smith, S. & Hollywood, J. S. (2013). *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations.* RAND Corporation. Online: https://doi.org/10.7249/RR233

Saravia, E. (2022). Prompt Engineering Guide. *GitHub*. Online: https://github.com/dair-ai/Prompt-Engineering-Guide

Stuart, R. D. (2013, February 5). Social Media: Establishing Criteria for Law Enforcement Use. *FBI Law Enforcement Bulletin*. Online: https://shorturl.at/intzO

Wallach, W. & Marchant, G. E. (2018). *An Agile Ethical/Legal Model for the International and National Governance of AI and Robotics.* Association for the Advancement of Artificial Intelligence. Online: https://shorturl.at/deHT7

Winfield, A. F. & Jirotka, M. (2018). Ethical Governance Is Essential in Building Trust in Robotics and Artificial Intelligence. *Philosophical Transactions of the Royal Society A Mathematical, Physical and Engineering Sciences, 376*(2133). Online: https://doi.org/10.1098/rsta.2018.0085

Privacy in an Age of Cybersurveillance[I]

Russell L. Weaver*

* Professor of Law, Distinguished University Scholar, Louis D. Brandeis School of Law, University of Louisville, Louisville, Kentucky, USA, e-mail: russell.weaver@louisville.edu

Abstract: This article provides an update on events since Edward Snowden, an employee of a National Security Agency (NSA) contractor, stole and released thousands of classified documents in 2013, revealing that the U.S. government was engaged in a massive secret cybersurveillance operation that was amassing information about people all over the world, including U.S. citizens. In the U.S., Snowden's revelations sparked a spirited debate regarding privacy rights, and in particular whether the U.S. cybersurveillance operation was appropriate in a democratic system. This article describes the scope of the cybersuveillance program, and examines how the courts and Congress responded to the Snowden revelations, and (in particular) how U.S. society evolved in the following years.

Keywords: privacy, secrecy, FISA, terrorism, FISC, cybersurveillance, search and seizure, Bill of Rights, reasonable expectation of privacy, Fourth Amendment

1. Introduction

Americans (and perhaps the entire world) were shocked in 2013 when Edward Snowden, an employee of a National Security Agency (NSA) contractor, stole and released thousands of classified documents (Shane, 2013b; Stanglin, 2013). As the documents were published by newspapers around the world, they revealed that the U.S. was engaged in a massive secret cybersurveillance operation that was amassing information about people all over the world, including U.S. citizens (Shane, 2013b; Stanglin, 2013).

The existence of the NSA's cybersurveillance program was remarkable given U.S. history. Many in the founding generation were highly distrustful of governmental power – even a democratically-elected one (Ketcham, 1986, p. xv). Illustrative were the views of Thomas Paine (1997) who argued that: "Society in every state is a blessing, but government even in its best state is but a necessary evil; in its worst state an

---

[I] This paper was first presented at the Forum on Privacy and Governmental Transparency (Ludovika University of Public Service) on 8 June 2023.

intolerable one."[1] Thus, even though the Declaration of Independence flatly declared that the power to govern derives from the consent of the governed, thereby implicitly rejecting the divine right of kings and articulating the basis for what would become a representative democracy based on principles from the Enlightenment (Bailyn, 1967, pp. 16–17), including the writings of John Locke (Paine, 1997, p. 3; Doernberg, 1985, pp. 52, 57, 64–65; Konig, 2008, pp. 250, 262), Thomas Paine (Shoenberger, 2010, pp. 431–432 note 6) and Baron de Montesquieu (Adair, 1957, pp. 344–345), the Framers of the U.S. Constitution sought to create a system where governmental power was limited and constrained. For example, the Constitution (Art. I, § 3) gave Congress only limited and enumerated powers, and it included Baron de Montesquieu's doctrine of "separation of powers" (Montesquieu, 2011, pp. 151–152). Citations to Montesquieu's theories regarding separation of powers, appear in the Federalist Papers (Beeman, 2012, no. 47) and the debates at the constitutional convention (Ketcham, 1986, pp. 85, 237, 249, 253, 260, 288, 339, 360) were frequently cited and discussed in early documents (Ketcham, 1986, pp. 159–160, 163, 166–167, 240, 247, 259–260, 357), and were interspersed throughout the U.S. Constitution (Art. II, Sec. 2, Clause 2).[2]

Given the history of the U.S., Snowden's revelations sparked a spirited debate regarding privacy rights, and in particular whether the U.S. cybersurveillance operation was appropriate in a democratic system (Calmes & Wingfield, 2013; Castle, 2013; Risen & Wingfield, 2013). While government has a legitimate interest in investigating suspected terrorists, as well as in shielding certain types of information (e.g. state secrets or information vital that is potentially damaging to national security or foreign relations) from public disclosure (Calmes & Wingfield, 2013; Castle, 2013; Risen & Wingfield, 2013),[3] many questioned whether the government should be involved in such broad-based

---

[1] This distrust was probably rooted in a variety of considerations. First, the American Revolution was precipitated by grievances against the British Government, and in particular alleged abuses by the British monarch. See, e.g. U.S. Declaration of Independence (July 4, 1776) listing grievances against the English King (although, in fact, some of the offenses had been committed by the British Parliament rather than the King). British officials had imposed restrictions on freedom of expression; see also Weaver (2019, pp. 190–191). In addition, they had conducted aggressive searches and seizures (Weaver, 2011). However, there was a second reason to be fearful of governmental power: many in the founding generation, or their ancestors, had emigrated from Europe to the American colonies in an effort to escape religious persecution. See *Everson v. Board of Education,* 330 U.S. 1, 8–9 (1947). Some European nations had created "established" religions, required everyone to support those religions, and aggressively persecuted those who tried to practice other religions.

[2] For example, even though Congress was given the power to enact legislation, the Constitution (Art. I, Sec. 7 [3]) required the President's signature as a prerequisite to enactment into law (unless Congress overrides the President's veto or the President allows the act to become law without his signature). The President has the power to appoint "Ambassadors, other public Ministers and Consuls, Judges of the Supreme Court, and all other Officers of the United States", but he can do so only "with the Advice and Consent of the Senate" (Art. II, Sec. 2, Clause 2). Although Congress and the President jointly enact legislation, the judiciary is frequently charged with interpreting that legislation, and determining its consistency with the constitutional structure. See *Marbury v. Madison,* 5 U.S. (1 Cranch) 137 (1803).

[3] See e.g. *United States v. Nixon,* 418 U.S. 683 (1974) ordering President Nixon to release information, but noting that confidentiality regarding the President's conversations and correspondence is generally privileged, and going on to note that this privilege is "fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution".

surveillance. As a result, when the Patriot Act,[4] which was enacted following the 9/11 attacks and provided the basis for the cybersurveillance program was up for renewal, many questioned whether it should be renewed (Hasan, 2015; Baker, 2014).

This article examines how the courts and Congress responded to the Snowden revelations, and (in particular) how U.S. society evolved in the following years.

2. Privacy and the Fourth Amendment

Although the concept of privacy is not explicitly articulated either in the U.S. Constitution or the Bill of Rights, privacy concepts played a prominent role in the formation of the U.S. governmental system. Interestingly, since the Framers of the U.S. Constitution (Art. I, § 8) had created a federal government with limited and enumerated powers, and had included separation of principles (Montesquieu, 2011, pp. 151–152),[5] they decided not to include a bill of rights in the Constitution, believing that it was unnecessary (and might even be harmful) (Bailyn, 1993, p. 808). This decision was met with vociferous opposition and threatened to derail approval of the Constitution.[6] In an effort to salvage the adoption process, a compromise was reached whereby the Constitution would be ratified "as is" (in other words, without a bill of rights), but the first Congress would be charged with proposing a list of rights.[7] As a result, the *Bill of Rights* entered the *Constitution* as the first ten amendments.

Included in the Bill of Rights were protections for a variety of rights, including protections against "unreasonable searches and seizures". The new Americans were motivated to demand these protections by abuses that occurred during the British colonial period. British officials had routinely used Writs of Assistance that allowed them to do no more than specify the object of a search, and thereby obtain a warrant allowing them

---

[4] USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) codified in various sections of the United States Code. The bill was formally entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001".

[5] For example, even though Congress was given the power to enact legislation, the Constitution (Art. I, Sec. 7 [3]) required the President's signature as a prerequisite to enactment (unless Congress overrides the President's veto or the President allows the act to become law without his signature). Likewise, although Congress and the President jointly enact legislation, the judiciary is frequently charged with interpreting that legislation, and sometimes in striking it down. See *Marbury v. Madison,* 5 U.S. (1 Cranch) 137 (1803). Moreover, many powers, such as the foreign affairs power, are shared between the President and Congress. See *United States v. Curtiss Wright Export Corp.,* 299 U.S. 304 (1936). For example, the Senate is charged with ratifying treaties, which the Constitution charges the President with the power to negotiate and make (U.S. Const., Art. II, Sec. 2 [2]), but only the entire Congress can declare war (U.S. Const., Art. I, Sec. 8 [11]), and the President is integrally involved in other foreign affairs issues as well. See *United States v. Curtiss Wright Export Corp.,* 299 U.S. 304 (1936). In addition, the Framers created different terms of office for different officials so that a single election could not dramatically shift the course and direction of government (U.S. Const., Art. I, Sec. 2 [1]). See Ketcham, 1986, p. xv. "Also, mindful of colonial experience and following the arguments of Montesquieu, the idea that the legislative, executive, and judicial powers had to be 'separated,' made to 'check and balance' each other in order to prevent tyranny, gained wide acceptance."

[6] See *McDonald v. City of Chicago,* 561 U.S. 742 (2010); *Wallace v. Jaffree,* 472 U.S. 78, 92 (1985) White, J., dissenting.

[7] Ibid.

to search any place where the goods might be found (see Weaver et al., 2021, p. 64),[8] without limit as to place or duration.[9] Colonial officials had also used "general warrants" that required them only to specify an offense, and then left it to the discretion of executing officials to decide which persons should be arrested and which places should be searched.[10] These British practices infuriated the colonists.[11] In response, the Fourth Amendment provided specific privacy protections to the people. It explicitly guaranteed the American people the right to be "secure" in their persons, houses, papers and effects. In addition, it implicitly banned general warrants and writs of assistance by providing that "no warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". In effect, the Fourth Amendment sought to create a balance between the societal interest in crime detection and prevention, and the individual interest in freedom from governmental intrusion as evidenced by the requirements of probable cause and particularity. Of course, the courts have subsequently created numerous exceptions to the warrant requirement, based on the idea that the Fourth Amendment only prohibits "unreasonable" searches and seizures (Weaver et al., 2021, chapter 4), but the Fourth Amendment's goal of protecting privacy remains unchanged.[12]

3. The Snowden revelations

Given the colonial history, and the Fourth Amendment protections, the Snowden revelations were striking in that they revealed a pervasive and aggressive governmental cybersurveillance program (Shane, 2013b; Stanglin, 2013). Snowden, who was stationed in Hawaii (Mazzetti & Schmidt, 2013), stole thousands of NSA documents involving the years 2007 to 2012 (Shane, 2013b; Stanglin, 2013), and fled to Hong Kong (Savage & Mazzetti, 2013). There, Snowden contacted a well-known journalist, who had written about Julian Assange and the WikiLeaks disclosures (Maass, 2013), and provided the journalist with an extensive interview and copies of thousands of classified documents disclosing the scope of the NSA surveillance program (Maass, 2013). Eventually, Snowden fled to Russia where he was granted asylum (Myers & Kramer, 2013).

Before the Snowden disclosures, while some may have suspected that the U.S. Government was spying on ordinary citizens, few envisioned the size or breadth of the surveillance operation which one commentator described as "breathtaking" (Shane, 2013b). The NSA employed 35,000 people (Shane, 2013b), had a budget of $10.8 billion

---

[8]   See *Virginia v. Moore,* 553 U.S. 164, 168–169 (2008); *Samson v. California,* 547 U.S. 843, 858 (2006); *Atwater v. City of Lago Vista,* 532 U.S. 318, 339–340 (2001).
[9]   See *Steagald v. United States,* 451 U.S. 204, 221 (1981); *Gilbert v. California,* 388 U.S. 263, 286 (1967) quoting *Boyd v. United States,* 116 U.S. 616, 625 (19).
[10] See *Virginia v. Moore,* 553 U.S. 164, 168–169 (2008); *Steagald v. United States,* 451 U.S. 204, 220 (1981); *Payton v. New York,* 445 U.S. 573 (1980).
[11] See *Carpenter v. United States,* 138 S.Ct. 2206, 2213 (2018). General warrants and writs of assistance were so "reviled" that they helped spark the Revolution; *United States v. New York Telephone Co.,* 434 U.S. 159, 180 (1977) Stewart, J., concurring in part and dissenting in part; see also *Wallace v. Jaffree,* 472 U.S. 78, 92 (1985) White, J., dissenting.
[12] See *Katz v. United States,* 389 U.S. 347 (1967).

per year (Shane, 2013b), and operated a worldwide surveillance operation (Maass, 2013). One commentator suggested that the staggering breadth of the program was motivated by the NSA's desire "not to miss anything", enhanced by a staggeringly large budget and the "near-invisibility" of the program from governmental scrutiny (Shane, 2013b).

In particular, the NSA was collecting vast amounts of electronic information, including telephonic information, phone calls, e-mails, text messages, records of credit card purchases and information from social media networks (Shane, 2013b). In addition, the NSA had hacked into foreign computers and installed software that allowed it to monitor actions on those computers (Shane, 2013b), and it had even issued a secret order to Verizon Wireless requiring that company to turn over its phone records (Maass, 2013). The NSA also developed a tool nicknamed "muscular" that it used to hack into Yahoo and Google data communication centres, thereby accessing hundreds millions of individual accounts belonging to both Americans and non-Americans (Gellman & Soltani, 2013). As a result, the NSA collected every e-mail sent through the Google or Yahoo systems or posted on the Google.doc system, involving some 1.8 million customer accounts and 182 million communication records over a single thirty-day period, including "to" and "from" e-mail information, as well as text, audio and video information (Mendoza, 2013). In addition, the U.S. Central Intelligence Agency (CIA) paid AT&T some $10 million per year for access to AT&T data files which allowed it to ask AT&T to search its database for information related to designated individuals (Angwin et al., 2015). However, because the CIA is prohibited from engaging in domestic spying on Americans, restrictions were imposed on the AT&T data collection process to protect American identities (Angwin et al., 2015). In theory, the NSA surveillance program was focused on obtaining access to communications of "foreign intelligence value", and on electronic communications that carried information pertaining to foreign intelligence targets (Mendoza, 2013). Whether this was actually true is unclear. In any event, the NSA was storing massive amounts of information for up to five years.

The NSA was even spying on foreign leaders, including the heads of allied nations such as Germany, France, Brazil, Israel and Japan (Mendoza, 2013), and had even monitored German Chancellor Angel Merkel's cellphone (Smale, 2013). In addition, the NSA had spied on United Nations Secretary General Ban Ki-moon, in advance of his visit to the White House, in order to gain access to his talking points for the meeting (Smale, 2013). When the spying on allies came to light, it produced anger and outrage with the Germans characterising the spying as "completely unacceptable (Smale, 2013) and French President Francois Hollande viewing it as "totally unacceptable" (Rubin, 2013).

Whether the NSA's surveillance operation was effective is unclear. Some argue that the NSA gathered so much information that it was simply unable to analyse or make effective use of all of the information it collected (Shane, 2013b). Indeed, some of the data involved languages that NSA analysts were not capable of reading or analysing (Shane, 2013b). The NSA defended its possession of this megadata on the basis that it gave the NSA the ability to quickly search and uncover data as needed (Shane, 2013b). One estimate suggests that as much as fifty percent of the surveillance reports delivered to President Obama each morning were based on NSA surveillance (Shane, 2013b).

4. NSA cybersurveillance and governmental accountability

Another important aspect of the NSA cybersurveillance program is that it was being conducted almost entirely in secret. Virtually no one would argue that the nation's search for terrorist activity (or, for that matter, general police operations) must be completely transparent. On the contrary, the government needs to protect its sources as well as its strategies and techniques. But, if the electorate is going to be able to control and rein in governmental authority, there must be some level of transparency so that the people are informed regarding the general scope of what the government is doing and exercise their right to rein in governmental abuses. The problem is that it managed to maintain a very high level of secrecy regarding the NSA's cybersurveillance operations so that the public was generally unaware of the size and scope of the government's surveillance operation. For example, the NSA issued National Security Letters (NSL) designed to banks, internet service providers and telephone companies (Dallal, 2018, p. 1115). These letters would order the recipient not to disclose the existence of the order to anyone, including and especially the American public and the target of the inquiries (their customers) (Dallal, 2018, p. 1116; Shane, 2013b; Stanglin, 2013). In a four year period, the NSA issued approximately 200,000 NSLs (EFF, National Security Letters).

Secrecy was further enhanced by the fact that governmental officials lied to the public regarding the nature and scope of that program. For example, President Obama assured the U.S. public that the program was not focused on ordinary U.S. citizens, but rather only on individuals who pose a terrorist threat to the United States and on communications of "foreign intelligence value" and foreign intelligence targets (Shane, 2013a; Mendoza, 2013). At one point, he boldly proclaimed: "Nobody is listening to your telephone calls" (Shane, 2013a). Likewise, the NSA declared that it was not storing private online or phone information except under limited circumstances: when it believed that the recording or transcript contained "foreign intelligence information", evidence of a possible crime, a "threat of serious harm to life or property", or shed "light on technical issues like encryption or vulnerability to cyberattacks" (Shane, 2013a). However, it soon became clear that this was not true. The NSA had established a huge data storage centre (taking advantage of the declining cost of data storage and advances in search software sophistication) (Shane & Sanger, 2013), and it was routinely collecting phone "calls and e-mails in and out of the country" (Shane, 2013a). As a result, even if Americans were not the intended targets of NSA eavesdropping, they routinely fell "into the agency's global net" (Shane, 2013a). NSA Director, James Clapper even lied to Congress about the program (The Editorial Board of the New York Times, 2014; Rosenthal, 2013; Savage & Shane, 2013). When he was directly asked whether the NSA was collecting "any type of data at all on millions or hundreds of millions of Americans", he flatly stated: "No, sir. Not wittingly" (Savage & Shane, 2013). Clapper later explained the lie by stating that it was the "most truthful" or "least untruthful" thing that he could say at the time (Rosenthal, 2013).

Although the NSA was often required to obtain search warrants, these warrants were issued by secret courts and the warrants and the court orders were classified as "secret" and

withheld from public scrutiny.[13] To the extent that individuals tried to challenge the government's cybersurveillance in court, the courts shielded the NSA against being required to divulge information.[14] In other words, it was extremely difficult for the public to ascertain the nature or scope of the operation, much less to hold governmental officials democratically accountable. Secrecy was enhanced by the fact that the Foreign Intelligence Surveillance Act (FISA) of 1978[15] provided that applications for search warrants would be governed by two courts whose orders were shielded from public view.[16]

5. Judicial restraints on the NSA's cybersurveillance program

One might have expected the federal judiciary to have restrained the cybersurveillance program, but that did not happen for a variety of reasons. In theory, the NSA's cybersurveillance was checked by the FISC (Foreign Intelligence Surveillance Court) which was given the power to oversee warrant applications. However, the FISC was a virtual rubber stamp for the NSA (Turner, 2018, pp. 995–996). The FISC heard applications for warrants *ex parte,* and it granted warrant requests in more than 99% of all cases over a thirty year period (Turner, 2018, pp. 995–996). During that time, the FISC denied only 11 warrant requests out of 33,900 applications (Turner, 2018, pp. 995–996). In 2012, the FISC did not deny any of the 1,856 applications (Turner, 2018, p. 996).

One might also have anticipated that the Fourth Amendment prohibition against unreasonable searches and seizures would have imposed a significant limitation on the NSA's cybersurveillance authority, but that did not happen either. Although the Fourth Amendment has generally provided the citizenry with substantial protections against "unreasonable searches and seizures",[17] the U.S. Supreme Court has struggled to deal with the problem of advancing technology like that being used by the NSA (see Weaver, 2011).

At the founding of the nation in the eighteenth century, the state of technology was far less advanced. At that time, since cybertechnologies did not exist, the Framers of the Fourth Amendment were concerned about actual physical searches of persons and places.[18] As a result, U.S. Supreme Court precedent tended to limit the Fourth Amendment's application to situations in which the police actually searched a person[19] or trespassed or intruded onto a "constitutionally protected area".[20] The Court's approach became problematic as technology advanced to the point that the police could reveal information without actually trespassing or intruding into a constitutionally protected area.

---

[13] See *Clapper v. Amnesty International USA,* 568 U.S. 398 (2013).

[14] Ibid.

[15] 50 U.S.C. § 1801 et seq.

[16] 50 U.S.C. § 105(a)(3) & (b).

[17] See e.g. *Arizona v. Gant,* 556 U.S. 332 (2009); *Kyllo v. United States,* 533 U.S. 27 (2001); *Florida v. Royer,* 460 U.S. 491 (1983); *Mapp v. Ohio,* 367 U.S. 643 (1961).

[18] See *Draper v. United States,* 358 U.S. 307 (1959).

[19] Ibid.

[20] See *Goldman v. United States,* 316 U.S. 129 (1942); *Olmstead v. United States,* 277 U.S. 438 (1928); *Ex Parte Jackson,* 96 U.S. 727 (1877).

The warning signs were evident by the beginning of the twentieth century. By that time, the development and use of electricity had led to technological innovations which allowed the government to invade privacy without actually entering protected spaces (see Weaver, 2011). By that time, the Court was being confronted by relatively crude technologies such as "detectaphones" (which allowed the police to hear through walls),[21] "spike mikes",[22] and wiretapping.[23] Adhering to eighteenth century principles, the Court held that the police were not engaged in a search except when they actually penetrated into a "constitutionally protected area", such as a home (e.g. in case of a spike mike which was inserted into someone's home in order to overhear conversations inside the home).[24] For the detectaphone (which simply allowed the police to capture sounds being emitted from within a room), or wiretapping (which tapped phone lines outside someone's home), the Court refused to hold that the use of such technologies to spy on citizens constituted a "search" within the meaning of the Fourth Amendment.[25]

By the early part of the twentieth century, individual justices were beginning to sound the alarm regarding the intrusive impact of new technologies on individual privacy. In *Olmstead v. United States,*[26] with a degree of prescience, a dissenting Justice Brandeis argued that the "progress of science [...] is not likely to stop with wire tapping", and may some day allow the government "without removing papers from secret drawers" to "expose to a jury the most intimate occurrences of the home".[27] Brandeis argued that rather than inquiring whether the government has intruded into a "constitutionally protected area", the courts should focus on whether government had trampled on the "indefeasible right of personal security, personal liberty and private property".[28] In *Goldman v. United States,*[29] a dissenting Justice Murphy relied on Brandeis and Warren's (1890) seminal article on privacy, to argue that the Fourth Amendment should be broadly interpreted to protect "the individual against unwarranted intrusions by others into his private affairs",[30] and that the Court should provide greater protection for individual privacy.[31]

Nearly a half a century would pass before the Court would earnestly attempt to come to grips with the intrusive possibilities of newer technologies. Finally, in its landmark decision in *Katz v. United States,*[32] the Court mapped out a completely new approach for handling advancing technologies under the Fourth Amendment. Instead of asking whether the police had intruded into a "constitutionally protected area" (which, of course, would still constitute a search within the meaning of the Fourth Amendment), the Court would

---

[21] See *Goldman v. United States,* 316 U.S. 129 (1942).
[22] See *Silverman v. United States,* 365 U.S. 505 (1961).
[23] See *Olmstead v. United States,* 277 U.S. 438 (1928).
[24] See *Silverman v. United States,* 365 U.S. 505 (1961).
[25] See *Olmstead v. United States,* 277 U.S. 438 (1928); *Goldman v. United States,* 316 U.S. 129 (1942).
[26] 277 U.S. 438 (1928).
[27] Ibid. 474. Brandeis, J., dissenting.
[28] Ibid. 474–475.
[29] 316 U.S. 129 (1942).
[30] Ibid. 136. Murphy, J., dissenting.
[31] Ibid. 139.
[32] 389 U.S. 347 (1967).

inquire whether the government had violated an individual's "expectation of privacy".[33] A concurring Justice Harlan essentially agreed with the Court, but argued that the expectation of privacy must be one that society recognises as "reasonable".[34] The Court ultimately adopted the Harlan formulation.

The *Katz* test seemingly expanded the Fourth Amendment's application to advancing technologies. In that case, Katz had made a phone call from a telephone booth, and the police overheard the conversation because of a listening device attached to the outside of the booth. Prior precedent enabled the prosecution to argue that there had been no intrusion into a "constitutionally protected area" because a phone booth was not a protected area (like a home). Moreover, the government had not "trespassed" into the phone booth because it had simply attached a listening device to the outside in order to capture sound waves emanating from the booth. Despite the absence of a trespass, the Court found that the government's use of the listening device involved a search because the government had violated Katz's reasonable expectation of privacy (REOP): "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[35]

After *Katz,* one might have assumed that the REOP test would be used to impose limits on technologically-based searches. In fact, the test did not provide much protection against the onslaught of technology (Weaver, 2011, pp. 1153–1227). Although the Court rendered some post-*Katz* technology decisions that were privacy protective,[36] the general thrust of the Court's REOP jurisprudence was largely unprotective (Weaver, 2011, pp. 1153–1227). The Court narrowly construed the REOP test in a way that provided little protection against electronic intrusions (Weaver, 2011, pp. 1153–1227). Indeed, in a number of cases, the Court found that individuals do not have a REOP even though a reasonable person might very well have concluded otherwise. For example, the Court held that individuals do not have a REOP in open fields (even if they are fenced and posted with "no trespassing" signs),[37] against helicopters hovering at low altitudes over their homes,[38] against surreptitious examination of garbage that they leave on the street

---

[33] Ibid. 351. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

[34] Ibid. 361. Harlan, J., concurring. "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as reasonable."

[35] Ibid. 352.

[36] See *Riley v. California,* 134 S. Ct. 2472 (2014). Holding that the police may not search the electronic contents of an individual's smart phone, incident to arrest, despite precedent suggesting that the police can search "closed containers" as part of such a search; *Kyllo v. United States,* 533 U.S. 27 (2001) holding that the use of Forward Looking Infrared Technology to determine the amount of heat emanating from a home (in order to determine whether the owner might be using lights to grow marijuana in his attic) constituted a "search" within the meaning of the Fourth Amendment.

[37] See e.g. *Oliver v. United States,* 466 U.S. 170 (1984). "Open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance."

[38] See e.g. *Florida v. Riley,* 448 U.S. 445 (1989); *California v. Ciraolo,* 476 U.S. 207 (1986); *Dow Chemical Co. v. United States,* 476 U.S. 227 (1986).

for the garbage collector,[39] against canine sniffs designed to uncover whether a passenger is carrying illegal drugs in a suitcase,[40] or against the use of ground tracking devices that are used to follow their movements[41] (except when the device is used to uncover information about the inside of a home[42] or the police commit a trespass in installing the device on a vehicle[43]).

Perhaps the most restrictive limitation came from the notion that there is no REOP for information that is "voluntarily conveyed to a third party".[44] In *Smith v. Maryland,*[45] the Court held that the police did not violate an individual's REOP when they installed a pen register that allowed them to mechanically record all of the phone numbers dialled by Smith. The recording was done at the phone company rather than through an intrusion into the individual's home. The Court held that an individual has no "legitimate expectation of privacy" in things that he "voluntarily turns over to third parties", including to the phone company's mechanical equipment.[46] Likewise, in *United States v. Miller,*[47] the Court held that an individual did not retain a REOP in his bank records while they were held by the bank.[48] Finally, in *Couch v. United States,*[49] the Court held that a client could not claim a REOP in documents held by his accountant.[50]

If literally applied, the "voluntarily turned over to a third party" doctrine creates a gaping hole in the Fourth Amendment, and means that the Fourth Amendment provides almost no protection against the NSA's massive surveillance operation. In a modern technologically-driven society, most information is conveyed through third parties. E-mails are routinely sent through Internet service providers (ISPs), and text messages are routinely sent through cell phone service providers like Verizon, AT&T and T-Mobile. Even phone calls are sent through phone companies. Of course, *Katz* itself involved a phone call placed through the phone company, and the Court concluded that Katz was protected by a REOP. However, in light of decisions like *Smith, Miller* and *Couch,* it is not clear that e-mails and text messages are accompanied by a REOP today.

---

[39] See, e.g. *California v. Greenwood,* 486 U.S. 35 (1988).

[40] See, e.g. *United States v. Place,* 462 U.S. 696 (1983).

[41] See, e.g. *United States v. Knotts,* 460 U.S. 276 (1983).

[42] See, e.g. *United States v. Karo,* 468 U.S. 705 (1984).

[43] See, e.g. *United States v. Jones,* 132 S. Ct. 945 (2012).

[44] See, e.g. *Smith v. Maryland,* 442 U.S. 735 (1979); *United States v. Miller,* 425 U.S. 435 (1976); *Couch v. United States*, 409 U.S. 322 (1973).

[45] 442 U.S. 735 (1979).

[46] Ibid. 774–775. "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."

[47] 425 U.S. 435 (1976).

[48] Ibid. 440. Noting that Miller could not assert either ownership or possession over the records since the bank was required to keep them pursuant to its statutory obligations.

[49] 409 U.S. 322 (1973).

[50] Ibid. 335. "There can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."

Since these early decisions, the Court has rendered some privacy protective REOP decisions,[51] but the Court has never completely overruled the third party doctrine. However, in *Carpenter* v. *United States*,[52] the Court suggested that the third party doctrine is not without limits. In that case, the police had reason to believe that Carpenter (and others) had been involved in some robberies, they proceeded to obtain cell tower information which revealed that Carpenter was in the vicinity of the places that were robbed at the time of the robbery. The Court held that the police decision to access such information involved a search within the meaning of the Fourth Amendment.[53] In addition, although Carpenter had voluntarily conveyed information to a third party (his cell phone provider through the cell tower), the Court viewed cell phone location data as distinct from normal third party cases: "While the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. When *Smith* was decided, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[54] As a result, the Court carved out an exception to the third party doctrine: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[55] Nevertheless, the Court did not flatly overrule the third party doctrine and even suggested that special rules might apply when national security is at issue.[56]

Even if the REOP test were expanded to the point where it could be used to challenge NSA cybersurveillance, potential litigants would incur standing problems. In order to bring suit, individuals must be able to establish standing in the sense of showing that they are suffering injury. In *Clapper v. Amnesty International USA*,[57] individuals who were likely targets of surveillance sought to challenge the NSA's data collection program. However, because of the secrecy that pervaded the NSA program, plaintiffs were unable to prove that they were actual targets of the NSA program. The Court concluded that, without such proof, they could not establish standing to sue.[58] Of course, the *Clapper* decision placed most plaintiffs in an impossible situation. In order to have standing to sue, plaintiffs must be able to prove that the NSA is subjecting them to surveillance. However, the government was going to great lengths to maintain secrecy and to preclude plaintiffs for knowing whether they are subject to surveillance. In *Clapper,* plaintiffs sought to obtain the necessary information by asking that the Government be forced to reveal, through

---

[51] See *Riley v. California,* U.S. (2014) prohibiting the police from going through an individual's cell phone incident to an arrest; *Kyllo v. United States,* U.S. (2013) a search occurs when the police use forward looking infrared technology to determine the amount of heat coming from a house

[52] 138 S. Ct. 2206 (2018).

[53] Ibid. 2216–2218.

[54] Ibid. 2218.

[55] Ibid. 2219–2220.

[56] Ibid. 2220. "We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security."

[57] 568 U.S. 398 (2013).

[58] Weaver, 2011, p. 1143. Citing *Monsanto Co. v. Geertson Seed Farms,* 130 S. Ct. 2743, 2752 (2010).

in camera proceedings, whether it was intercepting respondents' communications and what targeting procedures it was using (Weaver, 2011, p. 1149). The Court refused to require the Government to make this revelation (Weaver, 2011, p. 1149), noting that plaintiffs were required to establish standing by "pointing to specific facts", and that the Government was not required to "disprove standing by revealing details of its surveillance priorities" (Weaver, 2011, p. 1149). The net effect was that, because the government's surveillance program was super secret, plaintiffs had difficulty proving that they were under surveillance, and therefore they could not meet the case or controversy necessary to proceed with the litigation. So, judicial intervention against the NSA's cybersurveillance program was extremely limited.

6. Subsequent political developments

Perhaps the most interesting question is how the democratic process would react to the Snowden revelations. The people could demand that politicians act to rein in the NSA's cybersurveillance activities. As we shall see, the political response was rather feeble. It is not entirely clear why politicians did not react more aggressively. Perhaps politicians were concerned that terrorists might strike again, and that politicians who had acted to hamstrung the NSA's anti-terrorism activities would be blamed for the attack.

The first opportunity for a political response came when the Patriot Act, which provided the basis for the NSA's cybersurveillance program,[59] came up for renewal. The Snowden revelations provoked considerable debate regarding whether the Act should be renewed (Hasan, 2015; Baker, 2014), and Congress initially allowed the Patriot Act to expire.[60] However, Congress replaced it with the USA Freedom Act of 2015 (hereafter "Freedom Act"),[61] which imposed some restrictions on the NSA's cybersurveillance system (Steinhauer & Weisman, 2015; Shear, 2015).

Some commentators question whether the Freedom Act achieved the right balance between governmental authority and privacy.[62] The Freedom Act did a number of things. First, it placed restrictions on the ability of the NSA to gather so-called "megadata" (Carlson et al., 2016, p. 499). Previously, the NSA would collect and store large quantities of data, but (in theory at least) could only search that data when it could prove to a judge that it could link that data to terrorist activity (Berman, 2018, p. 79; Cole, 2015). Under the Freedom Act, the data would no longer be held by the government, but instead would be held by the companies that collected the data, and could only be accessed by the NSA when a judge found a reasonable suspicion of a link to terrorist activity (Cole, 2015). Second, the Freedom Act sought to increase transparency by removing the NSA's ability

---

[59] USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001) codified in various sections of the United States Code. The bill was formally entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001".

[60] USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 codified at 50 U.S.C. 1801 (2016).

[61] USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 codified at 50 U.S.C. 1801 (2016).

[62] See e.g. Cole, 2015. "In truth, the USA Freedom Act addresses only a small fraction of the NSA's dragnet surveillance operation, and will leave most of the problematic programs Edward Snowden disclosed untouched."

to prohibit the recipient of a subpoena from disclosing the existence of the subpoena (Cole, 2015). Finally, the Freedom Act provided that some opinions of the FISC should be made public (Steinhauer & Weisman, 2015; Shear, 2015). Effectively, the Act required declassification and summaries of surveillance court orders, where possible, and some reporting on the volume of surveillance requests (Cole, 2015).

Although the Freedom Act sought to rein in the NSA's cybersurveillance program, it is not clear that the Act struck the right balance. For example, although the Act prohibited the collection of megadata, the NSA could still access that data through the collecting companies based only on a showing of a "reasonable suspicion" of a link to terrorist activity (Cole, 2015). One commentator described that change as not "insignificant", and concluded that "it's hardly a radical reform" (Cole, 2015). Likewise, although FISC opinions are no longer completely withheld, it expressed concerned about how long it took to begin releasing FISC opinions, as well as the fact that they were heavily redacted, thereby reducing their value (Guariglia & Mackey, 2022).

Others have questioned the Act, suggesting that Congress could have gone farther toward transparency without compromising the first against terrorism. For example, one commentator complained that Congress deleted a provision of the Freedom Act that would have "required the government to inform us of how many Americans it collects information on each year" (Guariglia & Mackey, 2022). That commentator referred to such information as perhaps the "most important" since, "unless we are aware of the scope of what the government is doing when it spies on us, we are unlikely to be able to control it" (Guariglia & Mackey, 2022). The commentator concludes: "If we are to preserve our privacy in the digital age, we must insist on new legal constraints – including the transparency necessary to know whether the reforms we impose are working. Otherwise, the digital tracks of our lives will become increasingly transparent to a government that will be increasingly secretive about what it is doing in our name" (Guariglia & Mackey, 2022).

7. Conclusion

The Snowden revelations provoked a debate in the U.S. regarding the proper balance between the governmental (and societal) interest in rooting out terrorists, and the individual interest in privacy. Prior to the Snowden revelations, the NSA's cybersurveillance was conducted almost entirely in secret, and the American public was unaware regarding the nature and scope of the NSA's activities. The debate ultimately led to the adoption of the Freedom Act which placed some restrictions on the NSA's authority (e.g. it was no longer allowed to collect metadata), gave the public access to heavily redacted FISC opinions, and lifted a prohibition against recipients of NSL letters from discussing the existence of those orders.

Of course, the Freedom Act did not produce complete transparency regarding the nature or scope of the NSA's cybersurveillance program, and perhaps nobody thought that it would. There is a place for some level of secrecy in the fight against terrorism. Society's challenge is to find the proper balance between the fight against terrorism and the individual interest in privacy. It is not clear that the Freedom Act achieved that balance.

References

Adair, D. (1957). "That Politics May Be Reduced to a Science": David Hume, James Madison and the Tenth Federalist. *The Huntington Library Quarterly, 20*(4), 343–360. Online: https://doi.org/10.2307/3816276

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L. & Risen, J. (2015, August 15). *AT&T Helped U.S. Spy on Internet on a Vast Scale.* The New York Times. Online: https://shorturl.at/qN027

Bailyn, B. (1967). *The Ideological Origins of the American Revolution.* Belknap Press.

Bailyn, B. (Ed.) (1993). *The Debate on the Constitution: Federalist and Antifederalist Speeches, Articles, and Letters During the Struggle over Ratification. Part One: September 1787 – February 1788.* Library of America.

Baker, P. (2014, January 15). *Obama's Path from Critic to Overseer of Spying.* The New York Times. Online: https://shorturl.at/dfgMP

Beeman, R. (Ed.) (2012). *The Federalist Papers.* Penguin Books.

Berman, E. (2018). Digital Searches, the Fourth Amendment, and the Magistrates' Revolt. *Emory Law Journal, 68*(1), 49–94. Online: https://scholarlycommons.law.emory.edu/elj/vol68/iss1/2

Calmes, J. & Wingfield, N. (2013, December 17). *Tech Leaders and Obama Find Shared Problem: Fading Public Trust.* The New York Times. Online: https://shorturl.at/mtJL8

Carlson, J. D., Goodale, G. M., Quinlan, G. C., Suarez, S. L., Meyer, J. M., McHugh, R., Petty, K. A. & Weinstein, B. H. (2016). National Security Law. *The Year in Review. An Annual Publication of the ABA/ Section of International Law, 51,* 497–513. Online: https://shorturl.at/ostJU

Castle, S. (2013, December 25). *TV Message by Snowden Says Privacy Still Matters.* The New York Times. Online: https://shorturl.at/ghJL6

Cole, D. (2015, May 6). *Here's What's Wrong with the USA Freedom Act.* The Nation. Online: https://shorturl.at/qrL35

Dallal, R. (2018). Speak No Evil: National Security Letters, Gag Orders, and the First Amendment. *Berkeley Technology Law Journal, 33*(4), 1115–1146. Online: https://doi.org/10.15779/Z388911R16

Doernberg, D. L. (1985). "We the People": John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action. *California Law Review, 73*(1), 52–118. Online: https://shorturl.at/qARSY

Electronic Frontier Foundation (EFF) (s. a.). *National Security Letters.* Online: https://shorturl.at/dehG4

Gellman, B. & Soltani, A. (2013, October 30). *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.* The Washington Post. Online: https://shorturl.at/aDFJL

Guariglia, M. & Mackey, A. (2022, August 22). *Victory: Government Finally Releases Secretive Court Rulings Sought by EFF.* Electronic Frontier Foundation. Online: https://shorturl.at/mIOR8

Hasan, M. (2015, November 30). *Why I Miss George W. Bush.* The New York Times. Online: https://shorturl.at/glpT0

Ketcham, R. (Ed.) (1986). *The Anti-Federalist Papers and the Constitutional Convention Debates.* New American Library.

Konig, D. (2008). Thomas Jefferson's Armed Citizenry and the Republican Militia. *Albany Government Law Review, 1,* 250–291.

Maass, P. (2013, August 13). *How Laura Poitras Helped Snowden Spill His Secrets.* The New York Times. Online: https://shorturl.at/aoxQ2

Mazzetti, M. & Schmidt, M. S. (2013, June 9). *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance.* The New York Times. Online: https://shorturl.at/qwC28

Mendoza, M. (2013, November 21). *Reagan Order Led to NSA's Broader Spying.* The Ithaca Journal.

Montesquieu, Baron de, C. (2011). *The Spirit of Laws.* Cosimo Classics.

Myers, S. L. & Kramer, A. E. (2013, August 1). *Defiant Russia Grants Snowden Year's Asylum.* The New York Times. Online: https://shorturl.at/fuzW6

Paine, T. (1997). *Common Sense.* Dover Publications.

Risen, J. & Wingfield, N. (2013, June 19). *Web's Reach Binds N.S.A. and Silicon Valley Leaders.* The New York Times. Online: https://shorturl.at/nCDMR

Rosenthal, A. (2013, October 24). *Clapper and Carney Get Slippery on Surveillance.* The New York Times. Online: https://shorturl.at/owJP4

Rubin, A. J. (2013, October 21). *French Condemn Surveillance by N.S.A.* The New York Times. Online: https://shorturl.at/dhAFG

Savage, C. & Mazzetti, M. (2013, June 10). *Cryptic Overtures and a Clandestine Meeting Gave Birth to a Blockbuster Story.* The New York Times. Online: https://shorturl.at/dgkGT

Savage, C. & Shane, S. (2013, June 17). *N.S.A. Leaker Denies Giving Secrets to China.* The New York Times. Online: https://shorturl.at/evB69

Shane, S. (2013a, June 20). *Documents Detail Restrictions on N.S.A. Surveillance.* The New York Times. Online: https://shorturl.at/yPZ23

Shane, S. (2013b, November 2). *No Morsel Too Minuscule for All-Consuming N.S.A.* The New York Times. Online: https://shorturl.at/jmyB1

Shane, S. & Sanger, D. E. (2013, June 30). *Job Title Key to Inner Access Held by Leaker.* The New York Times. Online: https://shorturl.at/cdk08

Shear, M. D. (2015, June 4). *Limits Reshape Terror Laws, and Obama's Legacy: News Analysis.* International New York Times.

Shoenberger, A. E. (2010). Connecticut Yankee in Europe's Court: An Alternative Vision of Constitutional Defamation Law to New York Times v. Sullivan? *Quinnipiac University Law Review, 28,* 431–489. Online: https://shorturl.at/ejkqQ

Smale, A. (2013, October 23). *Anger Growing among Allies on U.S. Spying.* The New York Times. Online: https://shorturl.at/AG249

Stanglin, D. (2013, July 31). *Report: Snowden Says NSA Can Tap E-Mail, Facebook Chats.* USA Today. Online: https://shorturl.at/cioDT

Steinhauer, J. & Weisman, J. (2015, June 4). *Surveillance in Place Since 2001 is Cut Back Sharply; New Legislation Curtails Sweeping Monitoring of American Phone Records.* International New York Times.

The Editorial Board of the New York Times (2014, January 1). *Edward Snowden, Whistle-Blower.* The New York Times. Online: https://shorturl.at/fBFG2

Turner, S. (2018). The Secrets of the Secret Court: An Analysis of the Missing Party and Oversight of the Foreign Intelligence Surveillance Court. *Administrative Law Review, 70*(4), 991–1019. Online: https://shorturl.at/fgtxT

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193–220. Online: https://doi.org/10.2307/1321160

Weaver, R. L. (2011). The James Otis Lecture: The Fourth Amendment, Privacy and Advancing Technology. *Mississippi Law Journal, 80,* 1131–1227.

Weaver, R. L. (2019). *From Gutenberg to the Internet. Free Speech, Advancing Technology, and the Implications for Democracy.* (2nd edition) Carolina Academic Press.

Weaver, R. L., Burkoff, J. M., Hancock, C. & Friedland, S. I. (2021). *Principles of Criminal Procedure.* (7th edition) West Academic.

This page intentionally left blank.

Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act[1]

Domingos Soares Farinho*

* Assistant Professor, Faculty of Law, University of Lisbon, Lisbon, Portugal, e-mail: domingosfarinho@fd.ulisboa.pt

Abstract: The new EU Digital Services Act (DSA) is intended to regulate intermediary service providers, with particular attention to online platforms and search engines. The core activity of such platforms and engines is personal data processing, pursuant to the tasks of content moderation and recommendations. This means that regarding personal data, there is an interconnection between the GDPR and the DSA, and it is a matter of law to determine how they interact in the EU digital space. This paper endeavours to draw a comprehensive picture of how the GDPR and the DSA seek to provide better guidance on the adequacy and enforcement of personal data protection. It is argued that their relationship is best described as the DSA being the *lex specialis* vis-à-vis the GDPR, but this is somewhat blurred by instances where the latter is mostly complementing the former, such as 1. specific legal basis for data processing in compliance with new legal obligations for platforms; 2. a new articulation between both regulations concerning dark patterns; 3. new prohibitions on personal data processing; 4. new duties for the protection of personal data; and 5. a new ancillary institutional framework to regulate data protection by online platforms in collaboration with national data protection authorities.

Keywords: Digital Services Act, GDPR, data protection, personal data, content moderation, profiling

---

[1] This paper was first presented at the Forum on Privacy and Governmental Transparency (Ludovika University of Public Service) on 8 June 2023.

1. Introduction

Online platforms and online search engines[1] have become some of the most significant processors of personal data in the world (Dijck et al., 2018, p. 13; Taddeo & Floridi, 2017a, p. 1; Taddeo & Floridi, 2017b, p. 13; Kurtz et al., 2019, pp. 5059–5068; Kurtz et al., 2022) due to their growing importance in the digital economy and in our daily lives (see Turillazzi et al., 2023, p. 6). From a legal perspective, this phenomenon raises the question of how users' personal data can be protected without disproportionally encroaching upon the freedoms of online platforms and other users. Legal systems address this issue in different ways but in the EU, the Digital Services Act (DSA) is intended to ensure a fundamental rights-based approach to regulating online platforms (Recital 3), meaning that the protection of personal data plays a central role.

The DSA is part of the European Union's Digital Strategy[2] which encompasses wide-ranging legislation including the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Artificial Intelligence Regulation (AI Act), and the European Chips Act. The DSA aims to play a key regulatory function within the EU Digital Strategy; its purpose is to regulate information society "intermediary services"[3] with a special focus on "online platforms". The DSA builds upon the e-Commerce Directive of 2000,[4] in which the concept of "intermediary service" was already central, but the act has further refined these categories. In the Directive, there was a simple threefold distinction made between "service providers" consisting of 1. providers of mere conduit services, 2. providers of caching services and 3. providers of hosting services. While retaining this threefold distinction (with "service providers" now referred to as "intermediary services"), the DSA differentiates between two new sub-categories within hosting services – "online platform" and "online search engine" – and one additional sub-category within each: "very large online platforms" (VLOP) and "very large online search engines" (VLOSE)[5]. Each new category is subject to additional rules, leading to stricter regulations being applied at the top of the pyramid (see Figure 1 below).

Thus, online platforms and online search engines refer to specific categories within the broad range of information society intermediary services covered by the subject matter of the DSA [see Article 2(1)]. Specific Sections of the DSA[6] have been dedicated to legally defining online platforms, simply because the business model of such platforms (as defined by the DSA) makes them fully dependent on personal data as "user-generated content

---

[1]   This paper uses the definitions of "online platform" and "online search engine" in accordance with Article 3(j) and 3(i) of the Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (hereinafter, the DSA).

[2]   See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 final (Digital Single Market Strategy); see also: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.

[3]   See Article 3(g) DSA.

[4]   Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[5]   See Article 33 DSA.

[6]   See Sections 3 through 5 of Chapter III of the DSA.

(UGC)" (York & Zuckerman, 2019, p. 138; Hartmann, 2020). These platforms collect personal data and process and monetise it in exchange for a service: allowing personal data subjects, i.e. users, to share their content online. Thus, personal data, within the business model of online platforms and search engines can be seen as a specific type of content *submitted to* and *provided by* those platforms and engines, at least in most cases. This point is important for understanding that although in the field of online platforms, both from a legal and business perspective, *content* is the term preferred in most cases to describe and explain how these specific types of hosting services work, most of this *content,* being user-generated, should also be described as *personal data, submitted to* and *used by* online platforms and *made available* to a variable number of users. It should be added that the term "user" is being used here in the broad sense of Article 3(b), (p) and (q) of the DSA, which includes not only "users" in the sense of "registered users" who have undergone the account registration process, but also "users" as recipients of the service for the purpose of "being exposed to information" hosted and presented by the platforms and search engines.

Furthermore, as online search engines are treated in the same way legally speaking as online platforms,[7] all references to online platforms hereafter include online search engines, unless stated otherwise.
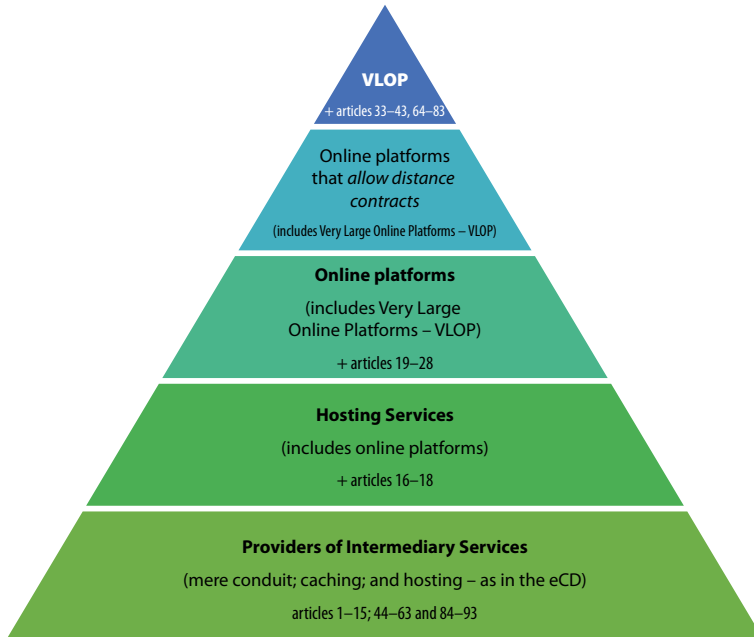

Figure 1.
The DSA regulatory pyramid

Source: Compiled by the author.

---

7   In the original proposal for the DSA, the Commission did not differentiate between online platforms and online search engines; this distinction was introduced at a later stage.

The DSA has to be applied with reference to the two principal EU laws on personal data protection within the digital domain, i.e. the GDPR and the e-Privacy Directive.[8] This means that the processing of personal data by online platforms is an activity which is closely regulated by EU law. Due to the close interconnection of the latter three pieces of legislation, it is only possible to determine what this legislation covers after careful analysis of the framework in place.

This paper endeavours to address this question by focusing on the specificities of the regulation of personal data processing by online platforms in the EU. In Section 2, we will review how the GDPR applies to online platforms, given that they qualify as personal data controllers under the Regulation. This will allow us (in Section 3) to better determine and analyse the specificities introduced by the DSA for cases where personal data are processed by online platforms. Thus in Section 3.1, we first examine the general data protection framework under the DSA, by way of its two defining topics: the legal basis for processing personal data introduced by the DSA and the implications in terms of liability when data is being processed by online platforms. In Section 3.2, we progress to considering specific issues raised by the DSA concerning personal data protection on online platforms. We first examine the obligation to protect personal data, especially with respect to content moderation as online platforms' core activity, and then progress to automated processing of personal data. In Section 3.3, we examine online interface design and organisation prohibitions, in order to understand how the DSA adds a further layer of protection over and above that of the GDPR. In Section 3.4, we analyse prohibitions on profiling in relation to advertising, minors and recommender systems. In Section 3.5, there is an examination of the institutional regulatory dimension of the DSA as a personal data protection law. Finally in Section 4, we comment on the way in which the DSA addresses protection of online platform users' personal data. The position presented here is that the DSA operates as *lex specialis* in the field of personal data protection with respect to online platforms. It not only introduces 1. specific legal basis for data processing in line with platforms' new legal obligations, but it also introduces 2. new prohibitions on the processing of personal data, 3. new data protection obligations, and 4. a new ancillary institutional framework to regulate data protection by online platforms in collaboration with national data protection authorities.

2. Applying the GDPR to online platforms

Under the GDPR, online platforms are just another type of controller [see Article 4(7)], i.e. they "alone or jointly with others, determine the purposes and means of the processing of personal data". This means that they fall under the material scope of the

---

8   Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

GDPR [Article 2(1)] and are required to provide lawful grounds for processing personal data [Article 6(1)].[9]

Personal data processing by online platforms occurs independently of any data subjects deciding to become *registered* platform users: online platforms also collect personal data from those data subjects who merely access the content shared on platforms, without registering for an account, and who, therefore, have no contractual relationship with the service.[10]

With respect to their users, online platforms are obliged to choose the applicable legal grounds for processing their personal data from the list set out by the EU legislator in Article 6(1) GDPR. An examination of this list reveals that, *a priori,* the legal basis foreseen by the legislator can be applicable to online platforms, depending on the circumstances and the services provided to users.[11] In case of online search engines, this appears to be more complex: depending on the specific service provided, it can be very difficult to accept the application of point (e) (reasons of public interest). The most common legal basis for online platforms to process personal data is either that such data is required in order to perform the contract between the user and the platform [Article 6(1)(b) GDPR], or the basis of user consent [Article 6(1)(a) GDPR]. In some instances, a platform's legitimate interests provide the basis for processing personal data [Article 6(1 (f)]. Nevertheless, it should be noted that given the legal definition of DSA for "online platform" and "online search engine", the personal data required to perform contracts for such services is very limited, especially in contrast to the quantity and uses of personal data required for their business model. As we shall see below, the DSA foresees some cases where it is necessary to process personal data in order to comply with the Act itself, thus falling under Article 6(1)(c).

No matter which grounds online platforms are relying upon, such grounds are subject to the principle of purpose limitation [Article 5(1)(a) GDPR]. Each of the grounds set forth under Article 6(1) is specifically linked to the principle of purpose limitation, inasmuch as the purpose for which personal data are processed is limited by the scope of the legal basis provided by the legislator. Consent [Article 6(1)(a)] depends on the purpose presented to the data subject; the scope of performance of a contract [Article 6(1)(b)] determines a purpose for the processing of personal data; legal obligations [Article 6(1)(c)] entail specific purposes and not others; the vital interests of users [Article 6(1)(d)] determine the precise purposes for which personal data are processed; the pursuit of certain public interests [Article 6(1)(e)] determines the purpose of personal data processing; and legitimate interests [Article 6(1)(f)] lead to different balancing outcomes depending on the purpose chosen.

Above and beyond the lawful grounds laid down in the GDPR, online platforms are always required to rely on consent in order to process personal traffic data for the "purpose of marketing electronic communications services or for the provision of value-added

---

9 Online platforms and search engines may also be qualified as processors, but this would have to be ascertained for each specific case; see Article 4(8) GDPR.

10 See, for instance, Facebook Privacy Policy, version of 2023.12.12.

11 For instance, Meta considers that it may process personal data based on any of the lawful grounds foreseen under Article 6(1) of the GDPR. See: https://shorturl.at/coBGZ

services" according to Article 6(3) of the e-Privacy Directive,[12] as well as for processing personal location data other than traffic data [Article 9(1) e-Privacy Directive].

Once an online platform begins processing personal data, under EU law it must comply with the remainder of the GDPR in the same way as any other controller or processor. This includes those cases where online platforms are joint controllers with other online services, such as traders[13] provided via the platforms. These cases pose significant challenges as they demand careful analysis of the so-called "boundary resources" (Kurtz et al., 2022) used by platforms to enable the provision of other services, such as apps made available to the users. Analysing the interconnection between the GDPR and the DSA allows us to better understand how protection of personal data applies specifically to online platforms.

Preliminary conclusion to section 2: online platforms and search engines under the DSA are also controllers (and may be processors) under the GDPR, and therefore are required to process personal data in accordance with one or more of the lawful grounds provided for in Article 6(1) GDPR.

3. Protection of personal data and the DSA

In this section, instances of overlap between the GDPR and the DSA are described, classified and analysed in order to provide a framework for online platforms' compliance with data protection duties. There is a distinction made between 1. the general framework of overlap, which includes content moderation and liability as two key pillars of the DSA which are linked to the GDPR, and specific areas of overlap such as 2. personal data protection obligations under the DSA, regarding content moderation and procedural rules, 3. online interface design and organisation prohibitions, 4. profiling prohibitions, and 5. the data protection regulatory approach taken by the DSA.

3.1. General framework: lawful grounds for processing and platform liability

There are numerous references to personal data in the DSA. It is not only referred to in general terms under Recital 10 and Article 2(4)(g), but is addressed in particular under 1. notice and action mechanisms (Recital 52); 2. online advertising (Recitals 68 and 69 and Articles 26, 39 and 46); 3. the protection of minors (Recital 71 and Article 28); 4. the traceability of traders (Recital 72); 5. the definition of active recipients (Recital 77); 6. recommender systems (Recital 94); 7. risk assessment for VLOP and VLOSE (Article 34); 8. research (Recitals 97 and 98); 9. codes of conduct (Recital 103 and Article 45); and 10. enforcement (Recital 148 and Article 40). Many

---

[12] Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[13] See article 3(f) DSA.

of these will be discussed below where they provide guidance on interpreting the relevant provisions.

Beyond explicit references to personal data, the DSA implicitly refers to it with respect to two important areas: legal grounds for processing and platform liability. These two areas are interconnected, because the legal basis applicable to personal data processing operations on online platforms give rise to liability in the event of a breach of the GDPR or of other rules on the protection of personal data.

3.1.1.   *Legal basis for the processing of personal data*

The GDPR determines the lawful grounds for the processing of personal data which are applicable to online platforms, as discussed above. The DSA elaborates on these grounds by laying down a set of legal obligations that online platforms are required to comply with and which involve the processing of personal data within the meaning of Article 6(1)(c). This set of obligations comprises: 1. compliance with orders to act against illegal content (Article 9); 2. compliance with orders to provide information (Article 10);[14] 3. management of notice and action mechanisms (Article 16); 4. statement of reasons (Article 17); 5. notifications of suspicion of criminal offences (Article 18); 6. compliance with obligations of traceability of traders (Articles 30 to 32); compliance with investigative and enforcement powers of the Commission in the case of VLOP and VLOSE (Article 40).

This means that where online platforms are concerned, it is necessary to take the DSA into account when assessing and applying the legal basis for the processing of personal data provided for under Article 6(1) of the GDPR. This is especially important because several DSA rules contribute to the application of the principle of purpose limitation.

3.1.2.   *Platform liability*

In addition to the possibility of personal data being used illegally by platforms – i.e. where no lawful ground exists for personal data processing or where prohibited profiling and targeted advertising takes place – it is also possible that third parties, such as traders and other platform users, can use personal data as illegal content, if they access such personal data through the online platform. Given that online platforms process personal data that they use themselves and allow third parties to use, it should be noted that platforms will remain liable for the breach of the GDPR, even where they are not aware that the personal data has been stored on the platform by another recipient of the service – circumstances which would exclude platform liability under the DSA pursuant to Article 6. It is important to distinguish clearly between 1. liability arising from the processing of personal data and the need to comply with the GDPR and other personal

---

[14]   Recital 34 specifically addresses this issue, noting that "the orders should be issued in compliance with Regulation (EU) 2016/679".

data protection legislation, and 2. liability that may arise for online platforms for personal data shared illegally by their users or for breaches of their due diligence obligations under the DSA.

The DSA maintains the rule of exempting online service providers from liability when illegal content is stored without the knowledge of the platform. This has been the rule in the EU (previously under Articles 12 to 14 of the e-Commerce Directive) since 2000 (Farinho & Campos, 2022, pp. 331–348). It is now laid down under Articles 4 to 6 of the DSA (Farinho, 2022, pp. 75–103), although the DSA has added a set of due diligence obligations with which platforms have to comply. This means that online platform liability differs depending on whether it concerns liability for breach of the GDPR or liability for breach of the DSA.[15] In the former case, online platforms are liable for breaches of the GDPR (see Article 82), for example: when personal data is processed without lawful grounds; processing principles are breached; security measures overlooked; or data transfers performed without specific lawful grounds; among other infringements related to online platforms' activities (Eifert et al., 2021, p. 1008). In the latter case, online platforms cannot be held liable for personal data shared by users unless the conditions under Article 6(1) of the DSA apply and the platform has breached their due diligence obligations. It is necessary to maintain this differentiation when applying the DSA.

However, there is one area where there may be an overlap of liabilities under the GDPR and the DSA – where platforms' due diligence obligations under the DSA concern personal data. The DSA gives one example in this area regarding the assessment of systemic risks by Very Large Online Platforms and Very Large Online Search Engines, under Article 34(1)(b) (see Buri, 2023, pp. 80–82).[16] Where VLOP and VLOSE fail to comply with this obligation, they may also be in breach of Article 24(1) and (2) and Article 31 of the GDPR.

Preliminary conclusions to section 3.1: as a general framework, the DSA provides for special cases of legal obligations as lawful grounds for personal data processing, elaborating on the general grounds provided for by Article 6(1)(c) of the GDPR. Data subjects/users, platforms and supervisory authorities should bear these special obligations in mind when determining whether there are lawful grounds for data processing, especially pursuant to Article 6(1)(c).

The DSA also regulates the liability of platforms in cases other than those arising from a breach of the GDPR as controllers (or processors). However, there is one area where liability can overlap, and this occurs when platforms fail to comply with due diligence obligations under the DSA in relation to the protection of personal data.

---

[15] See EDPS, "Opinion 1/2021 on the Proposal for a Digital Services Act", 2021, pp. 8 and 20.
[16] See Recitals 81 and 94.

3.2. Specific issues: obligations relating to the protection of personal data under the DSA

The DSA is mainly concerned with ensuring that online platforms comply with fundamental rights,[17] since privacy and the protection of personal data occupy a significant place under Articles 7 and 8 of the EU Charter of Fundamental Rights (EUCFR): "This Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated."[18] Online platforms are a particularly appropriate place to control the exercise of fundamental rights and, given this position, platforms do not only impact upon the exercise of these rights amongst their users, preventing or repressing violations to those rights, but in doing so, they may themselves breach fundamental rights (Egídio, 2022, pp. 217–238). For this reason, the DSA attaches particular importance to online platforms' moderating activities (Quintais et al., 2023): through content moderation, platforms can foster an environment that respects fundamental rights, but they can also restrict those fundamental rights (Gregorio, 2020). It is for this reason that the DSA has introduced procedural rules on how to moderate content and, in doing so, how to privately regulate and enforce fundamental rights (Bassini, 2019, pp. 182–197), including the protection of privacy and personal data (Quintais et al., 2023, pp. 881–911).

3.2.1. Content moderation and procedural rules

Content moderation is legally defined in Article 4(t) of the DSA: "The activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account." In order to moderate content, which, as emphasised above, is also personal data in most cases, it is necessary to process such content within the meaning of Article 4(2) GDPR. Given online platforms' operations and the use of automated systems, it is almost impossible to moderate content without processing at

---

[17] This concern echoes a similar concern of the United Nations regarding the respect of human rights by online platforms. See United Nations Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 2018. See also Land (2019, pp. 285–316).
[18] See Recital 9.

least some personal data.[19] It is up to those interpreting the law to determine when content moderation constitutes processing of personal data, which is why the due process guaranteed by the DSA toolkit is so important. The DSA aims at making content moderation transparent, pursuant to Articles 14, 15 and 35, in order to facilitate evaluation of compliance with fundamental rights, such as privacy and personal data protection. In the case of VLOP and VLOSE, this goal is clearly stated in the requirements of risk assessment procedures: pursuant to Article 34(1) and (2)(b) these kinds of service providers are required to assess the risk posed by their "content moderation systems" to "the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, *to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter,* to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter" (emphasis added). This means that the DSA requires online platforms to respect the right to privacy and the right to the protection of personal data in accordance with the GDPR, when applying their terms and conditions to users pursuant to Article 14(1) and (4).[20]

Content moderation, as envisaged by the DSA and viewed from the perspective of the GDPR and data protection, is as much an activity destined to protect the fundamental rights of users from other users and public authorities, as it is a means to protect users from the platform itself. This latter aspect is the essence of Article 14(4) of the DSA: any restrictions imposed on users by online platforms in the name of terms and conditions and enforced through content moderation mechanisms has to comply with fundamental rights (Quintais et al., 2023, pp. 881–911), and this involves protecting users both from public power and the power of the platforms.[21] Online platforms are called upon to perform a balancing act between the conflicting fundamental rights identified through content moderation mechanisms (Eifert et al., 2021, p. 1011). Content moderation includes taking down illegal content, as identified by the platforms, their users (including trusted flaggers pursuant to Article 22 of the DSA) and EU or EU Member States authorities. This is another area of overlap with the GDPR, given that orders to act against illegal content (Article 9 DSA) and notice and action mechanisms (Article 16 DSA) can be used to act against violations of the GDPR (as illegal content), or to exercise rights laid down in the latter regulation. An important example is the exercise of the right to erasure under the GDPR [see Article 17(1)(d)] vis-à-vis the notice and action mechanism against illegal use of a platform user's personal data [Article 16(1) DSA].

---

[19] See EDPS Opinion 1/2021 p. 10: "The EDPS wishes to underline that depending on the categories of data that are processed and nature of the processing, automated content moderation may significantly impact both the right to freedom of expression and the right to data protection."

[20] See Recitals 45 to 47.

[21] On the human/fundamental rights framework of online platforms regarding content moderation, see Jørgensen (2019, p. 181).

The DSA provides a set of procedural rules to underpin these balancing operations, but does not create new substantive rules to prevent or resolve such conflicts; rather, the DSA relies on a general reference to "illegal content"[22] as defined by EU and Member State law. Thus, the DSA focuses on procedural rules when dealing with content moderation. This is the case with 1. transparency reporting obligations, 2. notice and action mechanisms, 3. duty to state reasons, 4. use of internal complaint-handling systems and 5. out-of-court dispute settlements, as well as reliance on 6. trusted flaggers, 7. recommender system transparency, 8. traceability of traders, and, in the case of VLOP and VLOSE, 9. risk assessment and 10. measures to mitigate risks. This procedural toolkit also applies to the enforcement of the right to protection of personal data. The bottom line is that the DSA defines a specific type of personal data processing operation – content moderation – with the aim of ensuring that such processing complies with the fundamental rights to privacy and data protection and, consequently, with the GDPR.

Understanding content moderation as a specific type of personal data processing is important for those interpreting the law and for other legal practitioners, from platform lawyers to consumer association lawyers and, of course, supervisory authorities and judges. This is because content moderation's status as personal data means that content moderation due diligence rules under the DSA have to be applied in accordance with the GDPR, and any breach may also entail a breach to the GDPR.

3.2.1.1. Automated processing of personal data

Among the forms of content moderation, one type in particular deserves special attention from the EU legislator: automated processing. This is because this type of content moderation, which at least in its early stages does not involve human intervention, can lead to a range of problems ranging from classification errors to decision bias.[23] Concerning automated processing of personal data and especially in the case of content moderation, an interesting dialogue has been established between the GDPR and the DSA.

The DSA presupposes that online platforms use automated tools to some extent in order to moderate content (Recital 26). Under the GDPR, a particularly restrictive approach to automated personal data processing can be observed. Article 22(1) states that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[24] However, exceptions from Article 22(2) apply, which include: 1. where necessary to enter into or perform a contract, 2. authorisation by the Union or Member State law, or 3. explicit consent. This appears to mean that the data subject/user can object to the use of any content moderation tool by online platforms where it involves the processing of personal data, unless one of the

---

[22] For the DSA definition of illegal content see Article 3(h).
[23] See Article 29 Working Party, "Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679", adopted on 3 October 2017, and later adopted by the EDPB.
[24] See also Recital 71.

exceptions to Article 22(1) applies. As mentioned above, not all content moderation involves personal data processing, and this may explain the duties foreseen under Articles 14(1), 15(b), (c) and (e), 16(6) and 17(3)(c) of the DSA for online platforms to: 1. inform users, through their terms and conditions of any "policies, procedures, measures and tools used for the purpose of content moderation including algorithmic decision-making and human review"; 2. include in their transparency reports information on the use of automated content moderation tools;[25] 3. disclose the use of any automated means for processing or decision-making regarding notices of illegal content; and 4. include in their statement of reasons regarding any restrictions imposed on users "information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means".[26] This information is the only way for users to be able to exercise the right to object to such automated personal data processing and for administrative authorities to be able to assess compliance with the DSA.[27] Lastly, the DSA forbids decisions issued from the mandatory internal complaint-handling system to be based solely on automated means, pursuant to Article 20(6). Although these decisions may not relate directly to content moderation, they are connected with it inasmuch as most of these decisions are taken by the provider of the online platform following content moderation, as follows from Article 20(1) of the DSA.

 As part of this discussion, it is necessary to consider a third piece of legislation which will have the greatest impact on the automated processing of personal data in online platforms' content moderation mechanisms: the AI Act.[28] The Act had not yet been published at the time of this paper's submission for publication. However, during the negotiations among EU legislators, the issue of "consistency with the GDPR" was raised.[29] This is understandable as many online platforms use AI to perform content moderation operations. Insofar as these algorithms process personal data, they are subject to both the GDPR and the DSA, as well as the future AI Act (Pollicino & Gregorio, 2022, pp. 8–9).

 Preliminary conclusion to section 3.2: The focus of the DSA on content moderation and the procedural rules that frame such moderation should remind those interpreting the law that content moderation can be a type of personal data processing, and that, therefore, the procedural rules applicable to content moderation can function as specific rules applying to the obligations of the controller when personal data is processed. This is clear in the case of assessment of impact on fundamental rights, both in terms of content moderation and personal data processing. Therefore, GDPR and the DSA have to be applied in tandem whenever platforms are involved, and those interpreting the law will

---

[25] See EDPS Opinion 1/2021 p. 12.

[26] EDPS Opinion 1/2021 p. 12.

[27] See also Recitals 54 and 58 of the DSA; see Eifert et al. (2021, p. 1016).

[28] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021/0106(COD); latest version used (30 April 2024) available at: www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

[29] See European Parliament, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD))" of 20 April 2022, p. 157.

need to determine which obligations are relevant to content moderation as personal data processing, and how.

3.3. Specific issues: online interface design and organisation prohibitions

The DSA adds another layer of protection concerning manipulative or deceptive design, also known as dark patterns (Becker & Penfrat, 2023, pp. 56–57). As the EDPB reminds us, "[t]he GDPR's provisions apply to the entire course of personal data processing as part of the operation of social media platforms, i.e. to the entire life cycle of a user account",[30] and thus many deceptive practices in both the design and organisation of platform interfaces infringe the GDPR.[31] The DSA, while not laying down special rules which would affect those applicable in the GDPR – this is explicitly acknowledged under Article 25(2) of the DSA – provides a layer of rules of its own, prescribing, pursuant to Article 25(1) that platforms "shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".[32] In practice, this means that while the GDPR covers most deceptive patterns that involve personal data, especially given the guidance provided by the EDPB, the DSA will cover all remaining user interactions, where personal data is not present or where personal data is present but no provision from the GDPR covers that specific case. It is of utmost importance that further work is done by those interpreting the law, from scholars to supervisory authorities and courts, to determine whether and in what cases personal data may be protected by the DSA, rather than the GDPR, from the dark patterns in platforms' interfaces. That said, although the DSA provision regarding dark patterns most likely will not directly affect the protection of personal data, it may play a role in preventing or mitigating cases directly protected by the GDPR. This is something that must be taken into consideration by consumers and consumer associations when protecting the status of platform users.

> *Preliminary conclusion to section 3.3:* While not providing for special rules prohibiting dark patterns regarding the use of personal data, the DSA provides for a comprehensive prohibition on dark patterns regarding non-personal data that could work to prevent, mitigate or reinforce the protection of personal data against dark patterns covered by the GDPR, as well as in cases where the GDPR does not apply.

3.4. Specific issues: profiling prohibitions

Amongst other functions, the DSA reflects the EU's vision on how personal data is used by online platforms and endeavours to address those aspects of data processing, with

---

[30] See EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, adopted on 14 February 2023, p. 4.
[31] See EDPB Guidelines 03/2022 for several examples of online platforms' practices infringing the GDPR.
[32] See also Recital 67.

"profiling" centre stage as the main villain (Büchi et al., 2020). On the one hand, online platforms use personal data to personalise user experience, thus making the service more enticing, but also to monitor their actions and thus improve content moderation. On the other hand, such personal data and its findings can be used to offer better advertising services to companies, which in turn aim to reach potential clients more effectively. These two dimensions are clearly in the crosshairs of the DSA, and there was already an awareness of them prior to the enactment of the DSA. The European Data Protection Supervisor (EDPS), in his assessment of the DSA proposal, stressed that the three key areas of concern should be 1. content moderation; 2. online advertising; and 3. recommender systems.[33] Having analysed content moderation, online advertising and recommender systems will now be addressed.

3.4.1. Online advertising

Online advertising is the first domain in the DSA where one finds explicit and specific rules concerning the GDPR. Article 26(3) determines that "[p]roviders of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679". This rule was not in the EU Commission's original proposal, only being added after the amendments proposed by the EU Parliament.[34] This prohibition is composed of three elements. It addresses 1. targeted advertisement, 2. profiling and 3. sensitive personal data. In this sense, it combines three of the main concerns of the DSA and the GDPR.

Targeted advertising is not prohibited by either the GDPR or the DSA (except in the case of minors, see below) and the same can be said for profiling, although it raises several issues regarding online platforms in particular.[35] Given the high risk of targeted advertising on online platforms, the EDPB suggested the "prohibition of targeted advertising on the basis of pervasive tracking",[36] although this was not included in the final version of the DSA. Profiling is one of the major concerns of the GDPR,[37] warranting 1. a definition under Article 4(4) (Bygrave, 2020, pp. 125–131; Scholz, 2019, pp. 306–311; for profiling in general see Hildebrandt & Gutwirth, 2008), 2. specific rights to object to processing when profiling is involved, pursuant to Article 21(1) and (2) and 3. a right of the data subject "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly

---

[33] See EDPS Opinion 1/2021 p. 3.

[34] See European Parliament Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available online at: www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html

[35] See EDPB Guidelines 8/2020 on the targeting of social media users, Version 2.0 Adopted on 13 April 2021, pp. 5 and ff.

[36] EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 2.

[37] See EDPB Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018); see CJUE Decision C-252/21, *Bundeskartellamt*, 04.11.2023, ECLI:EU:C:2023:537.

affects him or her", under Article 22(1), with the exceptions provided for in paragraph (2).[38] On the other hand, sensitive data is highly protected in the DSA, its processing being forbidden by default under Article 9(1), with the exceptions in paragraph (2). This means that prior to the DSA and under the GDPR, online platforms could indeed perform targeted advertising based on profiling if one of the exclusions in Article 9(2), namely consent, applied. Thus, the rule in Article 26(3) of the DSA is a specific rule concerning the processing of sensitive personal data for targeted, profiled advertising. It can be said that whereas the GDPR and the e-Privacy Directive did not prohibit profiling based on personal data or the processing of personal data for targeted advertising – instead providing for the right to object [Article 21(2) GDPR] or consent-only advertising [Article 6(3) e-Privacy Directive] – the DSA now prohibits both when sensitive data is involved.[39] Taking into account that online targeted advertising relies heavily on sensitive data to profile users and better target ads, this was a compromise by the DSA legislator to prevent a complete ban on targeted advertising.[40]

This rule is especially important as a tool to fight dark patterns on online platforms (Valcke et al., 2022, p. 61). As can be read in Recital 69: "When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups."[41]

3.4.2. *Protection of minors*

A similar rule to that of Article 26(3) DSA can be found in Article 28(2) regarding the protection of minors: "Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor." Following the EDPB,[42] the DSA legislator again prohibits targeted advertising, in this case towards minors, if profiling based on their personal data is taking place. The subjective scope of the rule is narrower than that of Article 26(3) DSA, although wider in its objective scope: the rule applies only to minors and not to any online platform user, but the prohibition now extends to all targeted advertising based on the profiling of any personal data and not only that of a sensitive nature within the meaning of Article 9(1) of the GDPR.

There is no reference to minors in the GDPR, "children" being the preferred term of the legislator to address the concerns relating to minors. However, the two words do not have the same legal meaning. Minors in all EU legal systems are those data subjects who,

---

[38] On interpretative problems arising from Article 22(1) see Binns and Veale (2021, pp. 319–332).
[39] See Recital 68.
[40] Calling it a "half-baked restriction", see Becker and Penfrat (2023, p. 58).
[41] See EDPB Guidelines 03/2022 pp. 25 and 42 for some examples concerning advertising.
[42] See EDPB, "Statement on the Digital Services Package and Data Strategy", p. 3.

because of their age, do not yet have full legal capacity, even if the legal age of full capacity varies from country to country.[43] This difference is of relevance, not only because the DSA prefers the wording "minor", but because in the GDPR children can exert consent, regarding "information society services" when they are sixteen years old, or less if explicitly provided for under national law, according to Article 8(1).[44] This is an especially relevant provision of the GDPR as it is linked to Article 28(2) of the DSA: the DSA prevents online platforms from exposing children – as minors – to profiled targeted advertising, notwithstanding (and, one might add, especially in light of) the fact that children can consent to the use of online platforms from the age of 16.[45]

The legislator was cautious in the way it constructed this rule: 1. it applies not only in cases where online platforms know that the users are minors but also 2. in the cases where there is a "reasonable certainty" that the targeted users are minors. Such "reasonable certainty" does not demand that the online platforms process additional personal data in order to confirm whether the user is a minor [Article 28(3) DSA]. As mentioned in Recital 71, Article 28(2) "should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use".

3.4.3. *Recommender systems*

The DSA addresses recommender systems[46] regarding all online platforms under Article 27[47] but it lays down a specific rule for VLOP and VLOSE concerning the protection of personal data: "Providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679" (Article 38).[48] Again, profiling is targeted by the legislator and again following a suggestion by the EDPB.[49] In this case, profiling is not prohibited *per se*. What is prohibited is that online platform users be subjected exclusively to recommender systems based on profiling.[50] This means that the exclusive use of profiling as the basis for recommender systems is prohibited; this is another sign of the EU's stance on the harm that profiling can cause. In this case, this entails a restriction on the use of personal data, provided for outside of the GDPR, but in accordance with GDPR Articles 21 and 22.

---

[43] All EU Member States foresee eighteen as the age in which full legal capacity is acquired.

[44] For instance, under Portuguese law the age of consent regarding children is thirteen, pursuant to Article 16(1) of Law n.º 58/2019, of 8 August.

[45] See Recital 71 and its reference to "EU Better Internet for Kids strategy (BIK+)".

[46] For the legal definition of the DSA, see Article 3(s).

[47] See Recital 70.

[48] See Recital 94.

[49] EDPB Statement on the Digital Services Package and Data Strategy, p. 6.

[50] The EDPS not only suggested that "recommender systems should by default not be based on 'profiling' within the meaning Article 4(4) of Regulation (EU) 2016/679" but it also "strongly recommend[ed] to modify the requirement to opt-in rather than opt-out, making the option not based on profiling the default one". See EDPS, Opinion 1/2021, pp. 16 and 17.

Preliminary conclusions to section 3.4: The EU legislator appears to have used the DSA to go one step further in the treatment given by the GDPR to the profiling and targeting of data subjects. In all the instances where the DSA addresses these activities, it increases data protection by restricting profiling and targeting activities. It forbids targeted advertising using profiles based on sensitive personal data; it prohibits targeted advertising to minors based on profiling; and finally, concerning VLOP and VLOSE, it prohibits platforms from offering exclusively profiling-based recommender systems, obliging them to offer a non-profiled alternative.

3.5. The DSA data protection regulatory approach

In addition to the substantive and procedural rules analysed so far, there is a third important dimension to data protection in the DSA: the institutional regulatory framework (Eifert et al., 2021, p. 994). EU legislators have not only 1. created new national regulators – the Digital Services Coordinators[51] –, which have a duty to cooperate with each other pursuant to Article 58, but have also 2. envisaged a European Board for Digital Services, as an "independent advisory group of Digital Services Coordinators".[52] Last but not least, 3. the EU legislator has appointed the EU Commission as the enforcement authority for the DSA with respect to VLOP and VLOSE[53] (except for the provisions of Chapter III, Sections 1, 2, 3, where competence remains with the Digital Services Coordinators). Given the systemic risks posed by these very large service providers, the DSA requires that they perform a risk assessment covering, among other risks, "any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter" [Article 34(1)(b)]. Additionally, the DSA foresees a "crisis response mechanism" (Article 36) under which the Commission may define a set of measures to be applied by online platforms in order to mitigate or end a crisis.

The regulatory power conferred upon the new Digital Services Coordinators and the Commission is very extensive and focuses on the protection and enforcement of fundamental rights, where the protection of personal data is involved. As regards Digital Services Regulators, in Article 51 the DSA provides for 1. powers of investigation [paragraph (1)] and 2. powers of enforcement [paragraphs (2) and (3)]. The powers of investigation cover the inspection of content moderation procedures used by online platforms. As we have seen above, this involves the inspection of any personal data processing operations that may breach both the DSA and the GDPR. It follows that the regulatory institutional structure put in place by the DSA also regulates and enforces data protection when intermediary service providers are involved, as is the case with

---

[51] See Articles 49 to 51.
[52] See Article 61(1).
[53] See Articles 65 and ff. Also, on the status of the Commission as VLOP and VLOSE regulator, see Buri (2023, pp. 80–82).

online platforms. Here again, there is supposed to be an emphasis on the collaborative mechanism between the two institutional regulatory frameworks, especially between national data protection supervisory authorities and the new Digital Services Coordinators. When it comes to the Commission in respect of VLOP and VLOSE, the DSA also foresees extensive 1. investigatory powers (Articles 65 to 69) and 2. enforcement powers (Articles 70 to 76). Again to a great extent, this regulatory apparatus will have to focus on the protection of personal data,[54] in cooperation with the national supervisory authorities for the protection of personal data under the GDPR. This cooperation will be essential in order to adequately enforce personal data protection rules regarding online platforms:[55] many of the procedures foreseen in the DSA – pertaining to access to information via reports and other documents, giving reasons for the restriction of content, use of complaint and out-of-court dispute mechanisms – are a pre-condition for the use of complaint mechanisms under the GDPR and via the national data protection authorities. Information gathered from the DSA will support the procedures under the GDPR.[56]

Preliminary conclusions to section 3.5: In addition to the due diligence obligations set forth in the DSA, the institutional apparatus established by the DSA plays a significant role not only in platform regulation, but also in personal data protection. Given the fact that the digital services coordinators provided for in the DSA will act as special data protection regulators in addition to the general data protection regulators provided for in the GDPR, it becomes obvious that there will be a need for coordination. Such coordination needs to take place at three different levels: 1. within EU Member States between the GDPR supervisory authority and the DSA digital services coordinators, 2. among EU Member States concerning the result of internal coordination, and, regarding VLOPs and VLOSEs, 3. between the Commission and EU Member States. This results in a complex institutional system that will need to be carefully planned and monitored by each Member State and the Commission.

4. Conclusions

The main claim of the paper is that on the one hand, the DSA assumes the role of *lex specialis* vis-à-vis the GDPR, but on the other it also complements the GDPR; this calls for an analysis of 1. specific legal grounds for data processing in compliance with platforms' new legal obligations, 2. a new articulation between both regulations concerning dark patterns, 3. new prohibitions on personal data processing, 4. new obligations to protect personal data, and 5. a new ancillary institutional framework to

---

[54] See Recital 103.

[55] The EDPB has stressed the importance of this interplay and the lack of proper, formal mechanisms of cooperation. See EDPB, Statement on the Digital Services Package and Data Strategy, pp. 3 and 4; see also Jaursch (2023, pp. 95–96).

[56] This is especially important given the fact that most EU Member States have designated as their Digital Services Coordinator, in line with what had happened under the transposition of the e-Commerce Directive, their telecoms regulators and not their data protection supervisory authorities under the GDPR.

regulate data protection by online platforms in collaboration with national data protection authorities. Online platforms and search engines under the DSA are also controllers (and may be processors) under the GDPR and are, therefore, required to process personal data under one or more of the legal basis provided for by Article 6(1) GDPR. The DSA provides for special cases of legal obligations as legal grounds for personal data processing, thus elaborating on the general ground provided for by Article 6(1)(c) of the GDPR. Data subjects/users, platforms and supervisory authorities should bear these special obligations in mind when determining whether there are lawful grounds for data processing, especially pursuant to Article 6(1)(c). The DSA also covers cases of platform liability which differ from the liability arising from the breach of the GDPR as controllers (or processors), and this should be taken into consideration when assessing how platforms handle personal data. However, there is one area where liability can overlap, and this occurs when platforms fail to comply with due diligence obligations under the DSA regarding the protection of personal data. The DSA's focus on content moderation and procedural rules that frame such moderation activity must remind the interpreters of law that content moderation can be a type of personal data processing and, therefore, procedural rules applicable to content moderation may work as special rules concerning duties of the controller when processing personal data. This is clear in the case of fundamental rights impact assessment, both on content moderation and personal data processing. The GDPR and the DSA must, therefore, be used together, whenever platforms are involved and the interpreter wants to determine which duties apply (and how) to content moderation as personal data processing. Starting from this general framework, a set of specific areas where the DSA is linked to the GDPR were identified and analysed.

While not providing for special rules on the prohibition of dark patterns to be aligned with the provisions of the GDPR, it does provide for a comprehensive prohibition on dark patterns that may work to prevent, mitigate or reinforce the protection of personal data regarding dark patterns provided for by the GDPR or in cases where the GDPR does not apply.

The EU legislator seems to have used the DSA to go one step further in the treatment given by the GDPR to the profiling and targeting of data subjects. In all the instances where the DSA addresses these activities, it increases data protection by restricting profiling and targeting activities. It forbids targeted advertising using profiles based on sensitive personal data, it prohibits targeted advertising to minors based on profiling, and finally, concerning VLOP and VLOSE, it prohibits platforms from offering exclusively profiling-based recommender systems, creating a duty to offer a non-profiled alternative.

Finally, in addition to the due diligence duties set forth in the DSA, the institutional apparatus designed by the DSA plays a significant role not only in platform regulation but in its interplay with personal data protection. Given the fact that the digital services coordinators foreseen in the DSA will act as special data protection regulators in addition to the general data protection regulators foreseen in the GDPR, the need for coordination becomes obvious. This coordination will have to be done at three different levels: 1. within EU Member States between the GDPR supervisory authority and the DSA digital services coordinators, 2. among EU Member States concerning the result of internal coordination,

and, regarding VLOP and VLOSE, 3. between the Commission and EU Member States. This results in a complex institutional arrangement that must be carefully planned and monitored by each Member State and the Commission.

The analysis presented in this paper shows that personal data protection continues to exhibit a radiant effect stemming from the GDPR towards new legislation enacted by the European Union. The DSA is one of the most recent examples of this effect (as is the upcoming AI Act), and it is an especially important one as this regulation deals with everyday interactions on the Internet, through online platforms. Concerning data protection, the analysis performed showed that there are several areas where the GDPR and the DSA meet and the actors in the legal chain related to personal data protection compliance and enforcement can use the present work as a tool to interpret and apply the combination of GDPR and DSA provisions regarding the protection of personal data on online platforms. The analysis also shows, however, that there are some areas – like dark patterns, exercise of rights and institutional articulation – where the interaction between the GDPR and the DSA will require further elaboration from supervisory authorities, the EDPB, the new European Board for Digital Services, the Commission and the courts, with special emphasis on the CJEU. Further work of scholars and practitioners within a framework of the identified areas of interaction can undoubtedly help this endeavour.

Acknowledgments

References

Bassini, M. (2019). Fundamental Rights and Private Enforcement in the Digital Age. *European Law Journal, 25*(2), 182–197. Online: https://doi.org/10.1111/eulj.12310

Becker, S. & Penfrat, J. (2023). Still Useful. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implication*s (pp. 51–62). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Binns, R. & Veale, M. (2021). Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law, 11*(4), 319–332. Online: https://doi.org/10.1093/idpl/ipab020

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S. & Viljoen, S. (2020). The Chilling Effect of Algorithmic Profiling: Mapping the Issues. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105367

Buri, I. (2023). A Regulator Caught Between Conflicting Policy Objectives. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implication*s (pp. 75–90). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Bygrave, L. (2020). Commentary to Article 4(4). In C. Kuner, L. A. Bygrave & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 125–131). Oxford University Press. Online: https://doi.org/10.1093/oso/9780198826491.003.0010

Dijck, J. van, Poell, T. & Waal, M. de (2018). *The Platform Society. Public Values in a Connective World*. Oxford University Press. Online: https://doi.org/10.1093/oso/9780190889760.001.0001

Egídio, M. M. (2022). Social Networks and the Exercise of Fundamental Rights: Public Administration and the Digitalization of Fundamental Rights. In C. B. de Morais, G. F. Mendes & T. Vesting (Ed.), *The Rule of Law in Cyberspace* (pp. 217–238). Springer. Online: https://doi.org/10.1007/978-3-031-07377-9_12

Eifert, M., Metzger, A., Schweitzer, H. & Wagner, G. (2021). Taming the Giants: The DMA/DSA Package. *Common Market Law Review, 58*(4), 987–1028. Online: https://doi.org/10.54648/cola2021065

Farinho, D. S. (2022). Fundamental Rights and Conflict Resolution in the Digital Services Act Proposal: A First Approach. *e-Pública, 9*(1), 75–103. Online: https://shorturl.at/ijAQR

Farinho, D. S. & Campos, R. R. (2022). Models of Legal Liability for Social Networks: Between Germany and Portugal. In C. B. de Morais, G. F. Mendes & T. Vesting (Eds.), *The Rule of Law in Cyberspace* (pp. 331–348). Springer. Online: https://doi.org/10.1007/978-3-031-07377-9_17

Goldman, E. (2020). An Overview of the United States' Section 230 Internet Immunity. In G. Frosio (Ed.), *The Oxford Handbook of Online Intermediary Liability* (pp. 155–171). Oxford University Press. Online: https://doi.org/10.1093/oxfordhb/9780198837138.013.8

Gregorio, G. De (2020). Democratising Online Content Moderation: A Constitutional Framework. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105374

Hartmann, I. A. (2020). A New Framework for Online Content Moderation. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105376

Hildebrandt, M. & Gutwirth, S. (Eds.) (2008). *Profiling the European Citizen*. Springer. Online: https://doi.org/10.1007/978-1-4020-6914-7

Jaursch, J. (2023). Platform Oversight. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications* (pp. 91–106). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Jørgensen, R. F. (2019). Rights Talk. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 163–188). MIT Press.

Klonick K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review, 131*(6), 1598–1670. Online: https://shorturl.at/bnEO3

Kosseff, J. (2016). The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution Over Two Decades. *The Columbia Science & Technology Law Review, 18*(1), 1–41. Online: https://doi.org/10.7916/stlr.v18i1.4011

Kurtz, C., Wittner, F., Semmann, M. & Schulz, W. (2019). The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems. *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 52, pp. 5059–5068.

Kurtz, C., Wittner, F., Semmann, M., Schulz, W. & Böhmann, T. (2022). Accountability of Platform Providers for Unlawful Personal Data Processing in Their Eco-Systems – A Socio-Techno-Legal Analysis of Facebook and Apple's iOS According to the GDPR. *Journal of Responsible Technology, 9.* Online: https://doi.org/10.1016/j.jrt.2021.100018

Land, M. K. (2019). Regulating Private Harms Online: Content Regulation under Human Rights Law. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 285–316). MIT Press.

Pollicino, O. & Gregorio, G. De (2022). Constitutional Law in the Algorithmic Society. In H.-W. Micklitz, O. Pollicino, A. Simoncini, G. Sartor & G. De Gregorio (Eds.), *Constitutional Challenges in the Algorithmic Society* (pp. 3–24). Cambridge University Press. Online: https://doi.org/10.1017/9781108914857.002

Quintais, J. P., Appelman, N. & Ó Fathaigh, R. (2023). Using Terms and Conditions to Apply Fundamental Rights to Content Moderation. *German Law Journal, 24*(5), 881–911. Online: https://doi.org/10.1017/glj.2023.53

Scholz, P. (2019). Kommentar zum artikel 4 Nr. 4. In S. Simitis, G. Hornung & I. g. D. Spiecker (Eds.), *Datenschutzrecht. DSGVO mit BDSG* (pp. 306–311). Nomos.

Taddeo, M. & Floridi, L. (2017a). New Civic Responsibilities for Online Service Providers. In M. Taddeo & L. Floridi (Eds.), *The Responsibilities of Online Service Providers* (pp. 1–10). Springer. Online: https://doi.org/10.1007/978-3-319-47852-4_1

Taddeo, M. & Floridi, L. (2017b). The Moral Responsibilities of Online Service Providers. In M. Taddeo, L. Floridi (Eds.), *The Responsibilities of Online Service Providers* (pp. 13–42). Springer. Online: https://doi.org/10.1007/978-3-319-47852-4_2

Turillazzi, A., Taddeo, M., Floridi, L. & Casolari, F. (2023). The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications. *Law, Innovation and Technology, 15*(1), 83–106. Online: https://doi.org/10.1080/17579961.2023.2184136

United Nations Human Rights Council (2018). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

Valcke, P., Clifford, D. & Dessers, V. K. (2022). Constitutional Challenges in the Emotional AI Era. In H.-W. Micklitz, O. Pollicino, A. Simoncini, G. Sartor & G. De Gregorio (Eds.), *Constitutional Challenges in the Algorithmic Society* (pp. 57–77). Cambridge University Press. Online: https://doi.org/10.1017/9781108914857.005

Wischmeyer, T. (2020). What is illegal offline is also illegal online: the German Network Enforcement Act 2017. In B. Petkova & T. Ojanen (Eds.), *Fundamental Rights Protection Online* (pp. 28–56). Edward Elgar Publishing. Online: https://doi.org/10.4337/9781788976688.00012

York, J. C. & Zuckerman, E. (2019). Moderating the Public Sphere. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 137–162). MIT Press.

Transferring Digital Artworks on Online Market Platforms

Ágnes Juhász*, **Orsolya Lili Sztermen****

* Associate Professor, Department of Civil Law, Faculty of Law, University of Miskolc, Miskolc, Hungary, e-mail: agnes.juhasz@uni-miskolc.hu

** PhD Student, Ferenc Deák Doctoral School of Law, University of Miskolc, Miskolc, Hungary, e-mail: orsolya.sztermen@uni-miskolc.hu

Abstract: By writing this paper, the authors intended to answer questions raised by the transfer of digital artworks in the online space. At the beginning of the study, the basic expressions, including NFT digital artwork, will be explained. Then, it will be examined how these new forms of artwork can be treated by civil law. Although NFTs change hands daily, their legal nature, i.e. if they shall be deemed as things in the civil law sense, is unclear. If NFTs are treated as things, they can be a subject of ownership, and the provisions on the transfer of ownership rights shall be applied, which raises several further questions. According to another approach, NFTs embody the right to dispose, while there are other opinions as to which NFTs, following the model of bank account money, shall be deemed as claims facilitating the application of the provisions of the law of obligations. After reviewing the different approaches to the legal nature of NFTs, features of online auctions of NFT artworks will be introduced. Then, it will be examined if the platforms enabling online auctions fall under the scope of the recently adopted Digital Market Act and if so, which rules of the Act are applicable for them.

Keywords: NFT, non-fungible token, digital artwork, online auction, online market platform, gatekeeper, DMA

1. Preliminary thoughts

Seeing the emergence of regulatory development around the decentralised platforms as service providers also related to digital artworks, it is important to understand the forming legal framework stabilising non-fungible token (NFT) usage as a guarantee of any kind of digital asset such as digital artworks on online trading platforms. In the present scientific thesis, besides the terminology determination of digital artwork as a non-traditional type of artwork and its relevant trading platforms, we aim to collect and give a proximate explanation of NFT-based legal guarantee of the origin of digital assets in

the case of secondary market use. This type of special token, however, protects, individualises and for this purpose creates a digitally marketable position for digital artworks, but can be found and used in fully digitalised surfaces. To protect consumers of online market users, a now-forming regulatory framework is being under creation by the European Union governing bodies. Hereby we collect relevant regulatory changes and steps forward affecting the high-priced commercial appearance of 'NFTs' on secondary marketplaces which operate exclusively in the crypto-driven metaverse.

We attempt to analyse the European Digital Markets Act (hereinafter referred to as DMA)[1], which entered into force in May 2023, together with the Hungarian Civil Code (hereinafter referred to as HCC[2]) regulation of right in rem, being the basis of ownership change. Besides ownership right considerations, smart contracts as servants of NFT markets are also the focus of our research, namely the legally binding force of these not typical contract formulations created and activated also in the metaverse.

2. Clarification of terminology

The appearance of new technologies in the field of classical civil law requires professionals to be familiar with the operation of these digital mechanisms. However, these technologies have their own terminology which we shall know, understand and translate somehow for those who have no advanced IT skills. The problem of transferring ownership of digital artworks on online market platforms makes it necessary to be familiar with the content of several expressions which are basic regarding the topic. These expressions relate either to the phenomenon of digital artworks or the operation of goods, including artworks on any online market platform.

The followings explain the most important expressions to provide a theoretical foundation.

a) *Big data*. Big data refers to a large amount of data that originates from a large amount of information, and aggregates from different sources and are generated very quickly in terms of their properties. This information and data can be created by humans and machines, typically in the form of XML files, web pages, structured, partially structured, and unstructured data sets (Wang et al., 2016). Large companies such as PwC, IBM and KPMG provide a wealth of literature on big data analytics and business economics, as well as company-specific programmes for managing large data sets.[3]

b) *Blockchain*. Blockchain is a ledger, i.e. book of records, of all transactions, grouped in blocks, formulated with a (decentralised) virtual currency scheme (European Central Bank, 2015, p. 7). It is a kind of distributed ledger technology. It is a type of database that takes several records and puts them in a block rather than collating them onto a single sheet of paper. Each block is then 'chained' to the next block, using a cryptographic

---

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, pp. 1–66.

[2] Act V of 2013 on the Hungarian Civil Code.

[3] See for example PwC: Industry 4.0 – Building the digital enterprise, 2016, PricewaterhouseCoopers LLP.

signature. This structure allows blockchains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions. Each ledger keeps a copy of the digital database of all the transactions that have ever occurred (transactions record) which makes it possible for anyone to check the database, but, at the same time, no one can modify it.

A shared database for recording online transactions is called a ledger. The data structure is used in online distributed ledgers, storing and transmitting data in digital packets called 'blocks'. These blockchains use cryptographic and algorithmic methods to capture and synchronise data in the network. This is done in a way that data is also rendered immutable once it has been recorded. A blockchain is therefore a kind of record-keeping system that operates automatically, without any intermediary, such as a bank, credit institution, or accountant. The data recorded may be tangible, like a house, a car, or cash but can be intangible, like intellectual property, copyrights, patents, or know-how. The shared ledger may be accessible only to authorised members of the network, who can only use it for orders, payments, invoices and smart contracts.

At the EU legislative level, as part of the EU's digital finance package, a regulation was adopted in Autumn 2022[4] that regulates market infrastructures based on distributed ledger technology, to promote digital operational resilience and to implement digital financial services. The legislative package includes the potential and innovation of the digital revolution through European businesses, with the means to define and clarify definitions.[5] The movement of financial instruments issued through shared ledger technology will also be covered by the 2022 Hungarian legislation.[6]

c) *Cloud service.* A computing service is an interface, where two computing devices – hardware or software – or a computer and a human use it, meet and work together. There are three distinct types of cloud services: private, hybrid and public cloud.

d) *Crypto assets.* It is the main financial application of blockchain technology. According to the recently adopted European rules on markets in crypto assets (hereinafter referred as to MiCA),[7] crypto asset means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar

---

[4] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27.12.2022, pp. 1–79 (Hereinafter referred as to DORA).

[5] Regulation 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU, Regulation No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation No 648/2012, Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation No 236/201, Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[6] Act LXIX of 2022 on the amendment of laws affecting the financial sector, Article 12.

[7] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM (2020) 593 final, Brussels, 24.9.2020.

technology.[8] MiCA distinguishes three types of crypto assets. *Asset referenced token* means a type of crypto asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto assets, or a combination of such assets.[9] These tokens serve as a means of payment due to the stability of their value.

The main purpose of *electronic money token* (or e-money token) as a type of crypto asset is also to be used as a means of exchange, while it purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.[10] So, this kind of crypto asset is primarily a means of payment, but its value is pegged to a single fiat currency for reasons of stability. In addition to the differences, the e-money token has a few similarities in its functioning with the use of *electronic money,* insofar as they also act as electronic substitutes for coins and banknotes and are used for payment (for a comparison see Bacsó, 2016).[11] The holders of electronic money may require the electronic money institution to redeem their electronic money at par value for fiat currency at any time. This possibility, contrary to current practice, will also be available for e-money tokens after the entry into force of MiCA.

As the third type of crypto assets, MiCA refers to *utility tokens,* which, together with the above mentioned two other types of crypto assets, do not qualify as means of payment or exchange, i.e. do not serve financial purposes, but serve as digital access to goods or services available on DLT and are accepted only by the issuer of the token in question.[12] Therefore, this latter type of crypto asset is essentially linked to the functioning of the digital platform and digital services.

e) *Cryptocurrency.* A kind of crypto asset functioning as a currency, as a means of payment. It operates as a medium of exchange like the currency of coins or banknotes, but it exists only in digital (virtual) form, and it is secured by cryptography by using distributed ledger technology. In the case of a cryptocurrency, both the creation and the transactions are controlled by mathematical algorithms. Cryptocurrencies are a subset of digital currencies but can also be classified as alternative currencies or virtual currencies. A common feature of most cryptocurrencies is their decentralisation, i.e. they operate without centralised control (like the Internet), which allows them to be used as a cross-border currency. There are several kinds of cryptocurrencies nowadays. Cryptocurrencies can be clustered into two different categories: coins and tokens. Cryptocurrencies in the

---

[8] MiCA, Article 3(1), point 2.

[9] MiCA, Article 3(1), point 3.

[10] MiCA, Article 3(1), point 4.

[11] Electronic money is the monetary value represented by a claim on the issuer, stored electronically, including magnetic storage, issued upon receipt of funds for the execution of payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC and accepted by a natural or legal person other than the electronic money issuer. See Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267, 10.10.2009, pp. 7–17, Article 2, point 2. Article 6(1) point 16 of the Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises regulates electronic money as a payment instrument and defines it in accordance with the Directive.

[12] MiCA, Article 3(1), point 5.

first group use their independent blockchain (e.g. Bitcoin, Ether, Binance Coin, Solana), while others use another infrastructure of blockchain (e.g. Tether, Uniswap, Polygon).

f) *Digital artwork.* A digital file of metadata. It typically includes the following elements for identification when converted to a non-fungible token (NFT): title, author, size, description, edition number, etc. (Garbers-von Boehm et al., 2022, p. 15; about digital artwork (see Sztermen, 2022).

g) *Distributed ledger technology (DLT).* Technology that enables distributed ledgers to function and use.[13] This technology uses a distributed, decentralised, shared and replicated ledger which can be public or private, permissioned or permissionless, or driven by tokenised crypto economics or token less. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth.

h) *Intangible asset.* Assets that have an intangible form of representation but have an ideational and a market value. They directly serve the business activity for more than one year. Intangible means immaterial, non-material, intangible assets that are saleable, i.e. that represent an asset. Intangible assets are recognised by law for example as a form of fixed assets, next to tangible assets, financial fixed assets.[14]

i) *NFT.* It is a particular and encrypted unit of data on a digital ledger, typically a blockchain (Frye, 2021, p. 3). A cryptographic device with virtual or real content that uses blockchain to create a unique, non-replicable, fungible and tradable digital asset. A blockchain can be used for storage and registration, like a ledger found on the Internet. While cryptocurrencies such as Bitcoin, Ether, Solana, etc. are interchangeable, NFT is also interchangeable. They correspond to or represent (parts of) goods that are unique due to their characteristics, such as (digital or physical) works of art – or even real estate (Garbers-von Boehm et al., 2022, p. 13).

j) *P2P trading.* Peer-to-peer or person-to-person trading is a cryptocurrency exchange method that allows traders to trade directly with each other without the need for a third party or central intermediary to enter the transaction, either for registration or authentication. Instead of an automated engine, the online marketplace is a direct transaction after the product has been selected. There is more freedom to choose the needs, the exchange rate and the payment method, and the costs are lower. P2P platforms such as YouTube or UTorrent, which can be used for file sharing, often make illegal data, videos and files available to users, for example by causing copyright infringement.

k) *Smart Contract.* It is a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger.[15] A kind of computer protocol, which, by the application of blockchain technology, executes itself automatically, without the contribution of any other actor or intermediary (De Filippi & Wright, 2019, p. 33; Woebbeking, 2019, p. 107). The application of blockchain technology means that the transaction is automatically registered in a distributed

---

[13] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU, OJ L 151, 2.6.2022, pp. 1–33, Article 2(2).

[14] Act C of 2000 on accounting, Article 24(2).

[15] 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, Brussels, 23.2.2022, Article 2, point (16).

database. Thus, smart contracts are computer programs, linked to an electronic ledger that execute and settle transactions based on predefined conditions, since they transform the contract terms into computer code (Rohr & Wright, 2019, p. 473). These contracts which are independent from a central operator, guarantee the data owners and data recipients that the terms of data sharing will be respected (about the definition-making of smart contracts see Juhász, 2020).

l) *Tokenisation.* It is the process of transforming rights to tangible assets into tokens, i.e. the creation of digital analogues of real things. After this transformation, a token can act as an independent subject of civil transactions (Kulakova, 2022, p. 40).

3. Transferring the 'ownership' of digital artworks

In physical reality, the transfer of ownership of artworks takes place using property transfer contracts, sales, or, less frequently, gifts. However, it is common that before concluding the contract, i.e. the conclusion of the sales contract, the buyer is selected through a special competitive procedure (auction).

The issue of transfer of ownership of digital artworks raises several problems. The initial question is whether the digital artwork can be subject to ownership. If, according to civil law rules, a digital artwork cannot be included in the definition of the 'thing', then there can be no right of ownership on it, and therefore there can be no transfer of ownership. Answering this question is difficult: there are digital artworks that exist only in digital form, while others arose by the tokenisation of real physical objects, i.e. physically existing artifacts exist behind them. Thus, the NFT created in this way 'represents' the given asset in the virtual space and proves the ownership of that item (Kulakova, 2022, p. 42).

3.1. NFT digital artwork as the object of ownership

Regarding the NFTs including NFT digital artworks, it is necessary to answer the question of how an NFT can be interpreted: as a thing or as an embodiment of the right to dispose between different meta beings. Can the function of NFTs be deemed as a digital suitcase between metaverse objects?

Within the field of law in rem, 'thing' is one of the most fundamental concepts: it constitutes the indirect object of the legal relationship in rem, that is, what the direct object, the human behaviour is directed to. For this reason, the legislator must delineate the boundaries of the concept of thing within the framework of civil law, define what it considers to be a thing, and, because of this, what can serve as an indirect object of the legal relationship in rem. It should be noted, however, that the concept of a thing in the ordinary and legal sense is not the same: as a legal term, the thing serves to designate and define the object of rights in rem, so it has a narrower meaning than the concept used in everyday life (Juhász, 2023, p. 223).

According to Article 5:14(1) of the HCC, the object of ownership may be a physical object (thing) that can be taken into possession. However, paragraph (2) of the said article extends the rules on things to money and securities as well as to natural forces usable as things, while paragraph (3) provides for the appropriate application of the rules on things to animals, taking the provisions of acts establishing derogations reflecting their special nature into account.[16]

The possible revision of the boundaries of the concept of things delineated normatively by the legislature is a recurring issue of private jurisprudence. The concept of the thing described by the HCC is rather narrow and inflexible, which makes its application difficult regarding economic and social changes. The question of whether other private law 'phenomena' (e.g. intellectual property, corporate shares, bank account money, etc.) can be the subject of property law is repeatedly raised in the literature. Nowadays, the assessment of these phenomena is univocal: intellectual creations, regarding contemporary literary positions and judicial practice, do not qualify as things. Similarly, it can be stated about the share of a limited liability company that, although it is marketable and transferable as a set of intangible and pecuniary rights, it cannot be included in the category of things under the HCC. Bank account money, unlike cash in the form of banknotes and coins, is also not considered to be a thing.

Recently a new question arose: how to deal with the new phenomena emerging as a result of digitalisation (e.g. crypto assets, other digital assets, etc.) that cannot meet the criterion of possession required by civil law? The intensification of the digitalisation process, the emergence of artificial intelligence, the difficulties of placing the new phenomena into the civil law system, and the applicability of existing rules raise several new questions, to which the legislator will have to provide answers within the foreseeable future. The legislator shall provide about the legal status of digital data (Szilágyi, 2022a; Szilágyi, 2022b) and the private law treatment of crypto assets, in particular cryptocurrencies and NFT-based assets, which, however, cannot be given in the absence of regulation, solely based on different positions appearing in jurisprudence. Another question is whether the traditional conceptual framework may need to be revised, or expanded in any direction, or whether the current set of rules can be adapted appropriately to the new solutions.

In his recent study, Ákos Kőhidi (2022) outlined the classification of digital goods in virtual space in terms of property and contract law. Kőhidi referred to Christopher Cifrino, who presented three theories of property suggesting that the property rights of digital goods in the virtual world should be assessed based on the doctrines of contract law rather than property law. One of the theories introduced by Cifrino, based on the work of the English philosopher and political theorist, John Locke, is a theory of property that could provide a basis for property rights in virtual works since users of the platform spend hours acquiring an object. Cifrino (2014) also examines the scientific article of Margaret Radin (1982) with the title 'Property and Personhood', which argued the theory

---

[16] Cf. Act XXVIII of 1998 on animal protection (hereinafter referred to as APA). According to Article 5:30(1) HCC, the owner has the right to transfer or abandon ownership to someone else. On the other hand, Article 8 of the APA states that the ownership and keeping of animals kept in the vicinity of humans and dangerous animals may not be abandoned.

of regressive personhood, which addresses the relationship between persons and property in virtual worlds, is a theory that is not based on the contract alone.

As can be seen, determining the nature of NFT artwork is a difficult task. Nevertheless, according to the wording of the HCC, we have an opinion that *an NFT-based work of art cannot be regarded as a thing and therefore cannot be the object of property rights,* because such an artwork lacks spatial delimitation, physical appearance and the character of a 'corporeal object'. Instead of treating NFTs and NFT-based artworks as things, in our opinion, an approach that treats the NFT-based artworks as a kind of claim following the assessment of bank account money may be justified.

3.2. Transferring digital artwork in the metaverse

Traditional artworks which exist in physical form shall be deemed as 'things' according to the civil law rules, therefore, they can be the subject of ownership and the right of ownership can be transferred upon the provisions of property law. In the last decade, and especially after the Covid-19 pandemic, the transactions of artworks gradually moved to online space: artistic works change hands in the metaverse, on online auctions operated by different platforms.

Metaverses are online imitations of reality in which users participate in various activities and interact with each other using their virtual personalised avatars. The Metaverse, Web 3.0, and cryptocurrency are some of the emerging technologies that are transforming industries like gaming, online trading, cultural and educational work, and retail services. A lot of legal entities are developing their versions of their metaverse, e.g. the abovementioned Sotheby's, each with its unique set of network protocols, and cryptocurrencies. The crypto assets are used as means of exchange and store of value in these virtual worlds. Many metaverse blockchain projects are going on in the market which are constantly raising and competing for attention. Some of the top ones in 2023 are Decentraland (MANA), The Sandbox, Axie Infinity and Gala.

Recently, the trend of moving artwork auctions to online surfaces continued to strengthen particularly due to the appearance of NFT artworks, even if the nature of NFTs is currently unclear. In case of this category, transactions take place exclusively on online surfaces because of the nature of NFTs. On the one hand, sellers and buyers find each other on online marketplaces and can conduct their business directly. On the other hand, NFT artworks are offered for sale on online auctions organised by intermediaries like Christie's or Sotheby's or by others.[17] In 2021, Christie's was the first auction house that sold an NFT artwork and later, it hosted an NFT sale in Asia, accepting cryptocurrency, and taking live bidding in Ethereum,[18] even if they chose to conduct the bidding using their traditional online interface instead of on-chain at this time. Later, in Autumn 2022, the auction house launched the Christie's 3.0 platform[19] which allows it to carry out the entire auction

---

[17] Further details at https://superrare.com/; https://shorturl.at/JPW17; https://opensea.io/; www.niftygateway.com/; https://makersplace.com/

[18] Further details at www.christies.com/events/digital-art-and-NFTs/overview

[19] Further details at https://nft.christies.com/

process on the Ethereum blockchain. During this process, the bidder deposits an amount that fully covers his bid in a smart contract. On-chain auctions almost exclusively require bidding in native cryptocurrency, although there are some exceptions. (MakersPlace, for instance, allows one to make a bid either in cryptocurrency or in fiat money. In the latter case, a bid made in fiat currency will be converted into Ether in real time.) Besides Christie's, Sotheby's also developed its metaverse, launched in October 2021, where works of digital artists can be bought.[20]

4. Smart contract as a tool for the transfer of an NFT digital artwork

Increasingly, we hear the word 'artech' used to describe the possibility of using the latest technologies in the world of art, whether in the form of big data, software, or hardware. The one-way development of technology and art, their complementary nature, shows a one-way trend. Just as the digital world is gaining ground not only in imaging but also in commercial activities, smart contracts are helping the artech phenomena to achieve secondary market distribution. Big data and blockchain applied to art have grown into areas that are present in the focus of art lovers and potential future collectors.

The digital revolution has thus also reached the commercial activities of the art world. The storage and tracking of artworks' certificates, provenance and origin can be traced on a decentralised network. The benefits of non-replicable records in the form of metadata are that they can be used to store information about works of art in an authentic form, rather than having to keep or, where necessary, retrieve traditional paper documents. Authentic and complete authentication increases, and the value of the work of art and acts as an incentive for buyers. It also preserves the data of existing and NFT 'stamped' works, as well as newly created and NFT 'stamped' works. In this latter context, it is essential to set out some basic principles.

The tokenisation of digitally produced works, such as those produced with a digital camera or computer software technology, captured in digital space, which can be viewed on a device capable of displaying a digital image and managed in digital space, in the form of data that can be described as original and non-replicable, and which can be used and transferred, is a very useful and practical procedure for ensuring the marketability and transfer of ownership.

In case of NFTs, the token purchased is in fact a certificate of authenticity, which carries a link to the work and the owner's details. The image file itself is not delivered to the buyer, only a reduced version of the image is inserted into the user's cryptocurrency wallet. Crypto market stakeholders are working together to make the tokens more valuable over time. The secondary market for NFT artworks is also very strong, with 30% of SuperRare's turnover in April 2023, for example, coming from the resale of images. The smart contract stores the NFT token code, thereby implementing a record of the sale. There is no transfer of ownership of the underlying work in the traditional sense, only the

---

[20] Further details at https://metaverse.sothebys.com/

token, or the format of the command recorded in the smart contract, exchanges virtual ownership, whether tangible or intangible, which is unique to the token.

As already recorded in the first part of this paper, the NFT behind the digital artefact sold online is the heart of the sale. The tokenID is a smart contract, which is a combination of the smart contract that operates the NFT, describes it, and ensures its functionality as a tradable asset.

Smart contracts are used not only for transferring the NFT artwork but for making bids in an online auction. In those cases, where the online auction is carried out exclusively online, by using blockchain technology from the beginning to the end, on-chain bids are made in the form of a smart contract to guarantee the uniqueness of unchangeable transfer of ownership.

5. Regulating the operation of online auction platforms

As it was mentioned before, the nature of NFT is a central question from the point of view of civil law. However, these transactions take place *en masse* day after day regardless of whether NFTs are deemed as things or claims. Therefore, leaving this question aside, the online activity of auction houses and other intermediaries needs to be examined, since these are the surfaces where transactions on NFTs take place.

The operation of online platforms will be regulated in detail after the adoption of the DMA which aims to ensure the fair behaviour of the platforms. Although the trade of digital artworks represents only a quite narrow segment of the digital market, it gradually increases and due to the spread of NFTs these platforms can affect many users, therefore further examination may be justified.

5.1. Applicability of DMA provisions

According to Article 1(2) of the DMA, the provisions of the DMA shall apply to *core platform services* provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service. In the application of the DMA core platform services mean online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing services, online advertising services, including any advertising networks, advertising exchanges, and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed before.[21]

However, it is a basic question, if the online activity of auction houses can fall under the category of core platform services, can it be met with either of the subcategories of core

---

[21] Point (2) of Article 2 of the DMA.

platform services? Regulation 2019/1150 of the EU[22] determines the criteria to which an online service shall comply to fall under the scope of core platform service. Under Article 2(2) of Regulation 2019/1150, such service shall constitute information society services within the EU rules,[23] and allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where the transactions are ultimately concluded, and the service provides to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers. That is, the term 'online intermediation services' covers several types of online activities such as online stores, video-sharing portals, app stores, social networking sites, online payment sites, etc. Considering this, *the online activity of auction houses and other platforms which enable online auctions and serve as a place for selling and buying NFTs* including NFT artworks *shall be deemed as an online intermediation service.* Therefore, these activities fall under the scope of the DMA, and the provisions relating to core platform services shall be applied to them.

5.2. Online auction platforms as gatekeepers?

There are some large platforms that shall be qualified as gatekeepers, due to their strong market position. For those DMA sets out special obligations.[24] Precisely, these platforms are digital ones that provide an important gateway between business users and consumers. From their position, they can grant power to act as private rule makers, thereby creating a kind of 'bottleneck' in the digital economy. Since the beginning of May 2023, DMA applies according to which companies provide *core platform services.* The ones considered so shall notify themselves to the European Commission that they do meet all the thresholds determined by the DMA. This mandatory notification shall be made without delay and in any event within 2 months after those thresholds are met; at the same time, the undertaking shall provide the European Commission with the relevant information. DMA determines detailed and objective criteria for these large platforms – core platform service providers – to qualify as gatekeepers.

According to Article 3 of the DMA, an undertaking shall be designated as a gatekeeper, if a) it has a significant impact on the internal market; b) it provides a core platform service that is an important gateway for business users to reach end users; and c) it enjoys an entrenched and durable position in its operations, or it is foreseeable that it will enjoy such a position in the near future ('emerging gatekeeper').

Relating to the above-mentioned three criteria, further examination is needed. On the one hand, there are expressions that shall be explained. According to point (27)

---

[22] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, pp. 57–79.

[23] Cf. Point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), OJ L 241, 17.9.2015, pp. 1–15.

[24] Cf. Chapter III of the DMA.

of Article 2 of the DMA, 'undertaking' means an entity engaged in economic activity, regardless of its legal status and the way in which it is financed, including all linked enterprises, or connected undertakings that form a group through the direct or indirect control of an enterprise or undertaking by another. In criterion (b), business users and end users are mentioned. 'Business user' means any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or while providing goods or services to end user, while 'end user' means any natural or legal person using core platform services other than as a business user.[25]

On the other hand, the term 'significant impact on the internal market' shall also be interpreted. The term reflects the economic strength of the given undertaking due to which it can impact the operation of the market. Nevertheless, instead of giving objective content to this term, the European legislator defines three cases, in which it shall be presumed that the given undertaking satisfies the three requirements mentioned above, and therefore shall be deemed as gatekeeper. These presumptions are based on quantitative factors, taking into consideration the turnover of the undertaking, the monthly number of end users, and the yearly number of business users.[26]

The above-mentioned presumptions also have relevance regarding the European competition law. While the economic strength of an undertaking shall always be examined under competition law rules to determine if an undertaking dominates the market, in the case of gatekeepers it is not necessary. When an undertaking is qualified as a gatekeeper based on either of the presumptions, there is no need for defining the relevant market and examining the market position of the undertaking and the effects of its conduct on consumer welfare.

As it was mentioned before, undertakings that meet all the thresholds determined by the DMA shall notify the European Commission thereof.[27] After the entry into force of the DMA, the deadline for the notification was 3 July 2023. It is remarkable that for this time, only seven large platforms, Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft and Samsung notified the European Commission that they meet the thresholds to qualify as gatekeepers under the relevant provisions of the DMA. Another platform, Booking.com informed the Commission that it does not meet the thresholds yet but expects to meet the criteria at the end of 2023.[28]

Beyond the mandatory notification, the Commission has the right to designate a given platform as gatekeeper even if it does not meet the thresholds described in Article

---

[25] Points (20) and (21) of Article 2 of the DMA.
[26] Article 3(2) of the DMA.
[27] According to paragraph (68) of the preamble of the DMA, through mandatory reporting, gatekeepers should inform the Commission about the measures they intend to implement or have implemented in order to ensure effective compliance with those obligations, including those measures concerning compliance with the general data protection regulation of the EU [Regulation (EU) 2016/679], to the extent they are relevant for compliance with the obligations provided under these provisions, which should allow the Commission to fulfil its duties under this Regulation. In addition, a clear and comprehensible non-confidential summary of such information should be made publicly available while considering the legitimate interest of gatekeepers in protecting their business secrets and other confidential information. This non-confidential publication should enable third parties to assess whether the gatekeepers comply with the obligations laid down in this Regulation. Such reporting should be without prejudice to any enforcement action by the Commission at any time following the reporting.
[28] Further details at https://shorturl.at/jqKPV

2(2) of the DMA. This is only possible when the given platform meets each of the requirements of Article 2(2) of the DMA. In the course of this qualification procedure, the Commission takes different factors (e.g. the size of the undertaking, including turnover and market capitalisation, operations and position of that undertaking, structural business or service characteristics, etc.)[29] into consideration. Once a platform is qualified as a gatekeeper, Articles 6, 7 and 8 of the DMA provide for the obligations of the platform operator. The testing and qualification methodology described in the Annex may be updated and validated by the Commission considering current market developments.

After reviewing the criteria and procedure to qualify a given platform as a gatekeeper, we should answer the question of whether platforms enabling online auctions of digital artworks can be deemed as gatekeepers considering the quantitative and qualitative requirements determined by the DMA. Before answering, we should distinguish between platforms, which carry out auctions of different things including traditional and digital artworks (e.g. Opensea, Rarible, NBA Top Shop, Binance, VIV3, etc.), and those surfaces which organise auctions exclusively in the art sector (e.g. Super Rare, Nifty Gateway, Makersplace, KnownOrigin, Solanart, Async, Ronin). The transfer of an NFT digital artwork can take place in the same way on both platforms. Nevertheless, in the first case, the given platform reaches a larger number of end users or business users, therefore, it is more likely that it will meet the thresholds.

As we mentioned above, only seven large platforms notified themselves as gatekeepers until the deadline set by the DMA. Therefore, it can be stated that *online auction platforms enabling exclusively the transfer of digital artworks do not meet the thresholds determined by the DMA to qualify as gatekeepers.* Nonetheless, since the duty to notify the European Commission is an ongoing obligation of core service providers, it cannot be excluded that a digital artwork auction platform will meet the threshold sometime in the future. But not soon.

Another question, though, is how to assess when such a platform has met the threshold? Considering the criteria set out in Article 3(2) of the DMA, it shall be stated that both the turnover of an undertaking or the number of end users and business users can be assessed objectively since these have quantitative nature.

The monthly number of end users and the yearly number of business users can be determined relatively clearly since it is well-measurable by the different technical solutions. Nevertheless, buying and selling artworks either traditional or digital is a privilege of a quite narrow segment of society, therefore, presumably none of the platforms acting in the artwork market will meet the threshold to be qualified as gatekeepers.

Considering the other criterion, i.e. the turnover, it is obvious that the calculation of the turnover is more problematic. On the one hand, online auction platforms are operated by auction houses like Christie's and Sotheby's which, besides their online activity, still traditionally do their business when organising auctions with personal presence. For this reason, traditional and online sales of these auction houses shall be separated, because only online platforms providing core platform service fall under the scope of the DMA. Taking a step further, we should take into consideration that the sales taking place via online

---

[29] Cf. Article 2(8) of the DMA.

auctions are also different. There are auctions where bids can be made traditionally, off-chain, and in fiat currency, while there are other auctions, and this is an emerging trend of the above-mentioned auction houses, which pass off fully online, from the beginning to the end. In these cases, bids are made on-chain and, with a few exceptions, in cryptocurrency. In these cases, the calculation of turnover is complicated since the DMA set out the turnover threshold in EUR and does not contain any provision on the calculation of turnover. Nevertheless, it is presumable that the turnover can be calculated by the conversion of the given cryptocurrency to EUR.

6. Conclusory thoughts

To illustrate the above-mentioned problem, it is worth looking at the statistics on the sales of the largest auction houses Sotheby's and Christie's. According to the statistics, the total worldwide sales of auction house Sotheby's in 2022 reached approximately 8 billion U.S. dollars,[30] converted into euros this amount comes to EUR 7.3 billion.[31] Albeit the value of the total sales of Sotheby's shows that it could meet the thresholds set out by the DMA, it shall be mentioned that this value covers both traditional and online sales. According to another statistic,[32] the sales of NFTs on Sotheby's Metaverse show a gradually increasing trend and overall, from the launch of its Metaverse, the total sales of NFTs are nearly 18.7 million U.S. dollars, approximately 17 million euros. These latter transactions fully take place in the online sphere by using blockchain technology.

In 2022, the auction and private sales of Christie's generated approximately 8.41 billion U.S. dollars combined,[33] converted into euros this amount comes to EUR 7.6 billion. Within these sales, the company's online-only sales were 363 million U.S. dollars,[34] approximately 330 million euros.

As can be seen, calculating the turnover to assess if a given core platform service provider meets the threshold set out in the DMA is a complicated but not impossible task. Nonetheless, the number of sales of non-fungible tokens in the art segment shows an overall decreasing trend, therefore, it is unlikely that platforms selling exclusively NFT digital artworks would meet the thresholds soon.

---

[30] Further details at https://shorturl.at/fkIJQ
[31] All the above-mentioned sales were converted to euro on 10 July 2023.
[32] See www.statista.com/statistics/1282272/sotheby-s-metaverse-nft-sales-worldwide-by-auction/
[33] See www.statista.com/statistics/273256/revenue-of-christies-international/
[34] See www.statista.com/statistics/999436/christie-s-online-only-sales/

References

Bacsó, R. (2016). Virtuális valuta mint a modern kori pénzpiaci szabályozás kihívása [Virtual Currency as a Challenge of the Modern Financial Market Regulation]. *Polgári Szemle,* 12(1–3), 244–251. Online: https://shorturl.at/nuCF3

Cifrino, C. (2014). Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must be the Governing Paradigm in the Law of Virtual Worlds. *Boston College Law Review,* 55(1), 235–264. Online: https://shorturl.at/amqY1

De Filippi, P. & Wright, A. (2019). *Blockchain and the Law. The Rule of Code.* Harvard University Press.

European Central Bank (2015). *Virtual Currency Schemes – A Further Analysis.* Online: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Frye, B. L. (April 19, 2021). *NFTs & the Death of Art.* Online: http://dx.doi.org/10.2139/ssrn.3829399

Garbers-von Boehm, K., Haag, H. & Gruber, K. (2022). *Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized physical artwork.* Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies. Online: https://shorturl.at/hjySU

Juhász, Á. (2021). Intelligent Contracts – A New Generation of Contractual Agreements? *European Integration Studies,* 16(1), 41–53. Online: https://ojs.uni-miskolc.hu/index.php/eis/article/view/963

Juhász, Á. (2023). Hagyományos magánjogi megoldások – 21. századi kihívások [Conventional Private Law Solutions – 21st Century Challenges]. In Karlovitz, János Tibor (Ed.), *What Will Our Future Be Like?* (pp. 222–234). Sozial und Wirtschafts Forschungsgruppe.

Kőhidi, Á. (2022). A virtuális valóság pszeudoreáliáinak polgári jogi vizsgálata [Civil Law Analysis of Virtual Reality Pseudorealia]. *In Medias Res,* 11(2), 55–66. Online: https://inmediasresfolyoirat.hu/imr/article/view/251

Kulakova, O. S. (2022). Digital Art in the Light of NFT: Market Role and Legal Uncertainty. *Digital Law Review,* 3(2), 36–50. Online: https://doi.org/10.38044/2686-9136-2022-3-2-36-50

Radin, J. M. (1982). Property and Personhood. *Stanford Law Review*, 34(5), 957–1015. Online: https://doi.org/10.2307/1228541

Rohr, J. & Wright, A. (2019). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Market. *Hastings Law Journal,* 70(2), 463–524. Online: https://shorturl.at/bcv12

Szilágyi, F. (2022a). Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. I. rész [Who Owns the Digital Data? The Justification of Allocative Data Law in the Context of the Private Law (in Rem) Approach. Part I]. *Polgári Jog,* 7(9–10). Online: https://doi.org/10.55413/193.A2200501.POJ

Szilágyi, F. (2022b). Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. II. rész [Who Owns the Digital Data? The Justification of Allocative Data Law in the Context of the Private Law (in Rem) Approach. Part II]. *Polgári Jog,* 7(11–12). Online: https://doi.org/10.55413/193.A2200602.POJ

Sztermen, O. L. (2022). A digitális műalkotások megjelenési kérdései I. terminológiai problémák [Appearance and Legal Terminology of Digital Artworks: Part One: Thoughts on Terminology]. *Miskolci Jogtudó,* 6(3), 70–83. Online: https://shorturl.at/beoyP

Wang, G., Gunasekaran, A., Ngai, E. W. T & Papadopoulos, T. (2016). Big Data Analytics in Logistics and Supply Chain Management: Certain Investigations for Research and Applications. *International Journal of Production Economics,* 176(June), 98–110. Online: https://doi.org/10.1016/j.ijpe.2016.03.014

Woebbeking, M. K. (2019). The Impact of Smart Contracts on Traditional Concepts of Contracts Law. *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law,* 10(1), 106–113. Online: https://shorturl.at/btGJM

This page intentionally left blank.

E-Government in Nigeria

Can Generative AI Serve as a Tool for Civic Engagement?

Abdulrazaq Kayode Abdulkareem*

* Lecturer at the Department of Public Administration, University of Ilorin, Ilorin, Kwara, Nigeria, e-mail: abdulkareem.ka@unilorin.edu.ng

Abstract: This paper examines the potential for using generative artificial intelligence (AI) to boost civic participation in Nigeria's developing e-government ecosystem. Emerging generative technologies like ChatGPT demonstrate intriguing capabilities to make governance more interactive and engaging through conversational interfaces. Thoughtfully implemented AI tools could increase access and understanding of e-government, particularly for underserved groups. However, risks around bias, privacy, security and capability limitations pose challenges for public sector applications. Additionally, Nigeria's substantial digital divides and defective trust in government institutions hamper e-government participation currently. This paper analyses opportunities and limitations for applying generative AI to advance civic engagement given Nigeria's unique socio-cultural context. Findings suggest that while AI holds promise, targeted strategies focused on inclusion, accessibility, education and institutional legitimacy building are critical to realise benefits. Cautious optimism, human-centric design and responsible governance frameworks are needed to employ generative systems successfully. If challenges are addressed, AI could open innovative possibilities for energising civic participation. But further research and controlled pilot applications are required to determine optimal implementation.

Keywords: generative AI, ChatGPT, civil participation, digital literacy, e-government

1. Introduction

E-government initiatives, which are becoming increasingly common worldwide, aim to enhance public administration and services using digital technologies. These initiatives are designed to facilitate more efficient and effective governance, reducing bureaucratic red tape, and making government services more accessible to the public. One of the primary goals of many e-government programs is to foster civic participation and engagement (Abdulkareem et al., 2022b). This is achieved by providing citizens with

platforms and tools that allow them to interact with government agencies, voice their opinions, and participate in the policy-making process in a more seamless and straight-forward manner (Smith & Jamieson, 2006). By doing so, e-government initiatives can help to democratise the policy-making process, giving citizens a greater say in the deci-sions that affect their lives.

Recent advancements in generative AI, like ChatGPT, present exciting opportunities for revolutionising e-government services (Loukis et al., 2023). These systems can generate human-like text, potentially simplifying complex governance issues and making them more comprehensible for citizens. It may transform how citizens interact with government services, making them more accessible and user-friendly, and by way of providing a plat-form for clear and efficient communication, generative AI is capable of enhancing civic participation and engagement. It could also help in breaking down complex policy information into understandable language, thereby empowering citizens to make informed decisions (Vrabie, 2023).

One of its many merits consists in the ability of the generative AI to create automated chatbots that can interact with citizens in a natural, conversational manner. These chatbots can answer queries, provide information and guide users through various processes which improves the accessibility and efficiency of e-government services (Cantador et al., 2021; Mahapatra et al., 2012). In addition to chatbots, generative AI may also be used to develop interactive policy-guides which can present complex policy information in a simplified, easy-to-understand format. They can also adapt to the needs of individual users, providing personalised guidance based on each user's specific circumstances and queries (Balaji & Yuvaraj, 2019; Baldauf & Zimmermann, 2020).

In short, generative AI has the potential to significantly enhance two-way communi-cation between citizens and government agencies (Baldauf & Zimmermann, 2020; Chohan & Akhter, 2021; Tisland et al., 2022). It can be used to develop interactive tools that allow citizens to voice their opinions, provide feedback, or participate in decision-making processes, e.g. AI-powered chatbots could be used to collect citizen feedback on various issues, from public services to policy-proposals, and these chatbots could analyse and categorise the feedback, providing valuable insights to decision-makers. Moreover, generative AI could be used to create platforms for participatory decision-making, too (Ju et al., 2023). And these platforms are capable of enabling citizens to contribute with their ideas and opinions to the policy-making process, fostering a more inclusive and democratic form of governance. In effect, this results, then, in bridging the gap between citizens and their government, enhancing transparency, accountability and public trust in the process (Alexopoulos et al., 2019; Androutsopoulou et al., 2019; Androutsopoulou et al., 2021).

The above is well-illustrated by the early applications of generative AI in the public sector which have shown its potential to transform e-government services (Strauss, 2023; Valle-Cruz & García-Contreras, 2023). However, along the way to a successful applica-tion, data privacy is a key issue, as these technologies often handle sensitive information (Seböck et al., 2023). Measures must be taken to ensure data is used responsibly and securely; on the other hand, algorithmic bias is another serious concern (Wirtz et al., 2021; Wirtz et al., 2022). If the data used to train these AI systems is biased, the outputs

are also likely to be biased. It is crucial therefore to use diverse and representative training data and regularly audit the performance of AI to identify and mitigate any biases. Lastly, digital literacy is also of a significant concern. Not all citizens are equally comfortable or familiar with digital technologies. Consequently, these tools must be designed to be user-friendly and accessible, even for those with limited digital skills (Abdulkareem & Ramli, 2021).

The advent of generative AI technologies, like ChatGPT, presents therefore intriguing opportunities to revolutionise civic engagement within e-government participation ecosystems. This paper aims to examine the potential of leveraging these cutting-edge AI capabilities to enhance citizen participation and reinvigorate e-governance initiatives in Nigeria which has made strides in developing digital governance platforms (Abdulkareem & Ishola, 2016). However, citizen adoption and usage remain hindered by multiple barriers including lack of awareness, skills gaps, infrastructure deficits and eroding public trust. Generative AI tools demonstrate unique strengths that could help surmount some of these obstacles.

The present inquiry seeks to provide an analysis of both the opportunities and limitations associated with adopting generative AI technologies to reimagine civic participation within Nigeria's developing e-governance landscape. The core objective is to scrutinise how these emerging tools could be thoughtfully implemented to increase access, understanding and inclusiveness of digital governance channels for Nigerian citizens. By unpacking context-specific risks and rewards, the paper aims to offer insights to policy-makers on responsibly harnessing the potential of generative AI to foster more participatory and citizen-centric governance processes.

The intended contribution is to enrich discourse around the frontier applications of AI in the public sphere, anchored in the realities of Nigeria's socio-political environment. Ultimately, the analysis could help to shape strategies and governance frameworks for effective deployment of generative AI systems to bridge digital divides and energise civic engagement as the country strengthens its e-government architecture. Such evidence-based insights are crucial for developing countries aiming to embrace transformative technologies judiciously to propel more open, participatory and citizen-responsive governance models.

2. Methodology

To explore the potential of the generative AI for enhancing civic engagement in Nigerian e-governance, this study employed a multi-faceted qualitative approach. It conducted a comprehensive literature review on generative AI, e-governance and civic participation, analysed Nigeria's existing e-government policies and initiatives, and engaged in conceptual analysis grounded in the country's socio-political realities like digital divides, trust deficits and ethnic divides. Through this contextual lens, it critically examined opportunities and limitations of deploying generative AI for citizen participation, analysing factors like accessibility, inclusion and governance frameworks. Drawing from literature, policy-documents and contextual insights, the study developed a perspective on

strategically leveraging generative AI as a catalyst for citizen-centric digital governance in Nigeria while identifying key considerations, challenges and pathways for potential implementation.

3. Literature review

3.1. Generative AI and civic engagement

Generative AI technologies represent a paradigm shift in artificial intelligence, moving beyond simply processing and analysing existing data to creating entirely new content (Vrabie, 2023). These systems leverage advanced machine learning techniques, particularly large language models trained on vast datasets, to generate human-like outputs across various modalities like text, images, audio and code. By detecting patterns in the training data, generative AI models can produce novel, yet coherent and contextually relevant, content upon receiving prompts or inputs (Loukis et al., 2023). Systems like ChatGPT exemplify this generative capability in the realm of natural language processing. Powered by transformer-based architectures, these language models can engage in remarkably fluent written exchanges, understanding and responding to queries with nuanced, contextually appropriate text outputs that often exhibit human-like communication traits (Dwivedi et al., 2023). The ability to produce on-demand content that closely mimics human expression opens up transformative possibilities across sectors. In the civic sphere, generative AI could revolutionise how citizens interact with government, access information, and participate in decision-making processes through intuitive conversational interfaces and personalised content generation (Vrabie, 2023; Yang & Wang, 2023).

Prior research has underscored the immense potential of the generative AI to reshape civic engagement dynamics by introducing interactive, conversational interfaces between citizens and government bodies. A seminal study by Androutsopoulou et al. (2019) envisioned how AI-guided chatbots and dialogue agents could radically transform the nature of communication between the public and state institutions. By leveraging the ability of generative models to produce human-like responses, these conversational AI systems could simplify access to information and service delivery, acting as user-friendly gateways to complex governance processes. Moving beyond theoretical arguments, researchers have actively developed and tested generative AI prototypes for civic use cases. Notably, Cantador et al. (2021) implemented an AI conversational tool powered by language models to facilitate conversational search and exploration of open government data repositories. This system demonstrated how citizens could intuitively query vast open data resources through natural language interactions, potentially democratising access to public information reserves.

The pioneering studies showcasing generative AI applications for civic engagement have provided tangible proof-of-concepts that reveal the transformative potential of these technologies. By developing conversational AI agents and intuitive dialogue interfaces, researchers have demonstrated how generative models can bridge accessibility gaps that

have long hindered citizen participation in governance processes. These dialogue interfaces act as user-friendly gateways, empowering citizens to seamlessly navigate the often convoluted labyrinths of bureaucracy and engage transparently with governance functions. No longer constrained by complex terminology or hidden information architectures, the public can leverage these AI assistants to comprehend complex policies, access services, and have their voices heard through natural language interactions.

More so, the successfully prototyped use cases, such as Cantador et al. (2021) open data chatbot and AI Singapore's Ask Jamie virtual assistant (Ojeda, 2021; Shang et al., 2023), exemplify how generative AI models can collect and convey multifaceted governance information in easily understandable formats. By abstracting away complexity through fluent dialogues, these systems democratise access to the policy sphere, fostering a more participatory dynamic. Moreover, researchers like Baldauf and Zimmermann (2020) and Chohan and Akhter (2021) have outlined ambitious visions where voice-based generative AI could holistically enhance inclusivity and accessibility of citizen services. Interactive tools could collect feedback at scale and enable participatory decision-making by giving each citizen a conversational conduit to have their perspectives heard and factored into governance. As Vrabie (2023) notes, the core upside of generative AI in this context is its ability to engage in natural information exchange by way of simplifying complex concepts into easy-to-understand formats through back-and-forth dialogue. This capacity to bridge knowledge asymmetries could catalyse a paradigm shift towards truly citizen-centric digital governance models.

While the potential of generative AI to revolutionise civic engagement is promising, scholars have also raised valid concerns about the limitations and risks associated with deploying these technologies in the public sphere. A major issue highlighted by researchers like Wirtz et al. (2022) relates to governance challenges, including privacy violations, propagation of biases and lack of transparency in AI systems' decision-making processes. Given the sensitive nature of citizen data and the importance of maintaining public trust in governance institutions, the risks of privacy breaches and bias reproduction in generative AI outputs could undermine the very goals of fostering civic participation. If citizens perceive these systems as opaque or unaccountable, it could further erode trust and deter adoption. Dwivedi et al. (2023) have emphasised the critical need for responsible development practices to mitigate the dangers of generative AI inadvertently spreading misinformation or perpetuating harmful biases if not designed and implemented with rigorous safeguards. On the technical front, while generative models have exhibited impressive capabilities in engaging in back-and-forth exchanges, some experts like Androutsopoulou et al. (2021) argue that current systems still fall short in maintaining the coherent, open-ended dialogue required for substantive civic discourse. Limited context tracking and knowledge grounding are seen as bottlenecks that could undermine the depth and quality of citizen–AI interactions on complex policy matters.

Recognising these risks and limitations, several studies have explored frameworks and design principles aimed at mitigating potential pitfalls while unlocking the transformative potential of generative AI for civic engagement. For instance, Ju et al. (2023) conducted a discrete choice experiment to examine citizen preferences for specific social traits in AI chatbots, providing insights for developing more effective and citizen-centric conversational

agents. Meanwhile, Loukis et al. (2023) have outlined a comprehensive research agenda that systematically identifies key capabilities of generative AI, alignment with public values, associated challenges and potential directions for leveraging these technologies in conjunction with open government data and policies. Such holistic frameworks are crucial for guiding the responsible development and deployment of generative AI systems in the civic domain.

In conclusion, prior research has well-illuminated the unique capacity of generative AI to foster interactive citizen–government interfaces capable of demystifying complex governance processes and information through intuitive conversational experiences (Chui et al., 2023). However, realising this transformative democratic potential is contingent upon overcoming critical challenges through a complex, context-aware approach. Developing robust governance frameworks that safeguard against the propagation of bias, misinformation and privacy violations is paramount. Aligning generative AI systems with citizens' needs, preferences and socio-cultural contexts through citizen-centric design methodologies is imperative to ensure broad adoption and impact. Furthermore, continued research into enhancing dialogue coherence, context-tracking and knowledge grounding is crucial to facilitate substantive civic discourse beyond perfunctory interactions. Only by addressing these multifaceted challenges head-on can the immense promise of generative AI be harnessed as a democratising force that empowers citizens, catalyses inclusive participation, and combats the perpetuation of exclusionary practices or insidious misinformation campaigns. A balanced, nuanced approach sensitive to unique societal contexts can pave the way for generative AI to reshape civic engagement dynamics, fostering transparent, participatory and citizen-responsive governance models.

3.2. E-government in Nigeria

Nigeria's e-government efforts began in the early 2000s, and aimed at increasing efficiency and transparency in governance (Abdulkareem, 2015). A major early initiative was the establishment of the National Information Technology Development Agency (NITDA) in 2001 to provide strategic direction for ICT adoption. NITDA developed frameworks like the Nigerian e-Government Interoperability Framework to guide e-government systems development (Abdulkareem et al., 2022a). Key initiatives undertaken include online portals for accessing government information and services. The federal government has established portals such as *Nigeria.gov.ng* to provide centralised access to resources across ministries, departments and agencies. Individual agency portals like the Corporate Affairs Commission portal also enable online business registration and searches. Integrated identity management systems have also been a focus, such as the National Identification Number (NIN). The National Identity Management Commission was founded in 2007 to issue unique NINs to all citizens and legal residents. This foundational digital ID system aims to enhance service delivery across sectors. Additionally, there have been efforts to digitise government records and operations. NITDA's e-Government Masterplan seeks full automation of administrative functions and data. Initiatives like the Government Integrated Financial Management

Information System (GIFMIS) have digitised public financial management (National eGovernment Strategies, 2019).

However, uptake and adoption of these e-government platforms by Nigerian citizens remains low. A 2019 survey found only 28% of Nigerians accessed government web portals, citing multiple barriers to usage (Oni & Okunoye, 2019). A major obstacle is lack of awareness and digital literacy (Abdulkareem & Ramli, 2021). Many citizens, especially in rural areas, are simply not aware of e-government programs and portals. Those who face challenges in computer literacy and skills needed to effectively use digital services, and educational gaps exacerbated this problem. But unreliable digital infrastructure also impedes usage. For many Nigerians, access to affordable electricity, internet connectivity and digital devices continues to be a challenge (Abdulkareem, 2015). Frequent power outages disrupt access, while broadband penetration rates remain below 40% nationally. This urban–rural digital divide limits e-government participation. Additionally, years of ineffective governance have eroded public trust and confidence. Corruption scandals and perceptions of unresponsive bureaucracy have made citizens sceptical of e-government initiatives. Restoring faith in institutions will be critical. Cultural factors also come into play. Traditional norms and preferences for in-person transactions over digital channels persist.

Civic participation in governance also continues to be plagued by digital divide issues. Studies consistently show that wealthier, more educated Nigerians in urban centres have much greater access and ability to effectively use e-government services (Abdulkareem et al., 2022a). Rural areas and lower-income populations have, on the other hand, severe gaps in access and e-government usage. For example, a 2021 study found internet penetration rates of just 23% in rural zones compared to 65% in urban areas. Electricity access displays a similar divide which leads to stark inequalities in Nigerians' ability to leverage e-participation channels.

Obviously, the gaps are worsened by educational disparities as well. While higher literacy and digital skills allow savvier navigation of e-government platforms, those without such skills can find the interfaces overwhelming (Abdulkareem & Ramli, 2021). Initiatives to increase digital literacy among disadvantaged groups are therefore critical. These divides have thwarted efforts to broaden civic engagement online, and government initiatives to consult citizens on policy issues through portals have engaged only a thin slice of the populace. Typically, input comes predominantly from urban elites, marginalising rural and poorer Nigerians.

Nigeria's public sector has indeed recognised the need for innovation and has begun to explore the use of emerging technologies. For example, the National Centre for Artificial Intelligence and Robotics (NCAIR) is an initiative by the Nigerian Government to potentially leverage AI technologies to enhance civic participation and engagement.

4. Nigeria's socio-political landscape and opportunities for civic engagement using AI

Nigeria has a complex democratic history, having transitioned from military rule to a multi-party democratic system in 1999, ushering a new era of hope for democratic governance (Yusuf et al., 2018). However, the journey so far has been far from smooth with prevailing challenges testing the resilience of the country's democratic institutions. At the socio-political level, Nigeria's complex ethnic and religious tapestry has long been a double-edged sword (Ukiwo, 2006). On the one hand, the country's diversity is a source of immense cultural richness; on the other hand, it has frequently been a tinderbox for conflicts and tensions that threaten national unity (Oyedele, 2015). Historical grievances, disputes over resource allocation, and struggles for representation among the country's myriad ethnic groups have periodically erupted into violence, eroding social cohesion and trust in governing institutions (Omotoso, 2014). These fault lines had profound impact on civic engagement dynamics, with certain communities feeling marginalised or disenfranchised from mainstream political processes. Fostering inclusive platforms and rebuilding bridges across these divides will be critical for any e-governance initiative aiming to catalyse broad-based citizen participation.

Furthermore, Nigeria's institutional landscape has been marred by systemic issues like corruption, lack of accountability and inefficient bureaucracies, all of which have contributed to a deep-seated crisis of legitimacy in the eyes of many citizens (Abdulkareem et al., 2021). Decades of graft scandals, mismanagement of public resources and unresponsive governance have bred widespread cynicism and apathy towards state institutions, undermining the very notion of civic engagement. Restoring public trust and confidence in the integrity of governance systems will be a heroic task, but one that is essential for revitalising citizen participation. Robust institutional reforms, coupled with tangible demonstrations of transparency and accountability, could gradually help to rebuild the social contract between the state and its people. Nevertheless, on the cultural front, traditional norms and attitudes towards governance also play a role in shaping civic engagement dynamics. In many parts of Nigeria, there is a deep-rooted preference for in-person, face-to-face interactions and scepticism towards digital channels or platforms. This cultural predisposition poses challenges for the adoption and sustained use of e-governance tools, including those powered by cutting-edge technologies like generative AI.

Additionally, low levels of digital literacy and access to enabling infrastructure (reliable internet, electricity, devices) further exacerbate these cultural barriers, particularly in rural and marginalised communities (Abdulkareem, 2015). Bridging these divides through targeted capacity-building initiatives and ensuring equitable access to digital resources will be imperative. Ultimately, any efforts to leverage generative AI or other innovative technologies for catalysing civic engagement in Nigeria must be firmly grounded in the understanding of these socio-political, institutional and cultural realities. Technological solutions alone, no matter how advanced they are, cannot overcome entrenched systemic challenges or deeply ingrained societal dynamics.

Amidst these challenges, civil society organisations have emerged as advocates for democratic reforms, promoting transparency and accountability in governance, and

intensifying the voices of marginalised citizens. These organisations have served as observers and watchdogs, holding authorities accountable and championing the rights of citizens, playing a vital role in counterbalancing the democratic deficits that have plagued the country. Therefore, unpacking this context is vital for understanding both the immense need and potential pitfalls for leveraging generative AI to reinvigorate civic engagement. On the one hand, intuitive AI-powered platforms that simplify information and increase transparency could help rebuild trust and reconnect disaffected citizens with governance processes. On the other hand, generative models that facilitate two-way dialogue could provide citizens with accessible channels to voice their concerns and shape policies directly.

While generative AI does indeed represent a cutting-edge frontier of technological innovation, there is an evident risk that its introduction into Nigeria's civic engagement sphere could inadvertently exacerbate the existing divides and inequalities if they are not implemented thoughtfully. For instance, deploying generative AI virtual assistants that rely heavily on text-based natural language interactions may provide limited utility for citizens in rural areas with low literacy levels or limited digital skills. More so, deploying such AI systems within Nigeria's fraught socio-political landscape also poses unique risks, such as fuelling ethnic or religious conflicts or being weaponised to spread disinformation (Guenduez & Mettler, 2023).

There are also justifiable concerns around privacy and surveillance given the country's history of human rights abuses. One major concern highlighted regarding generative AI systems is their tendency to operate as inscrutable "black boxes", meaning that their inner workings and decision-making processes remain opaque and difficult to interpret, even as they produce outputs like natural language text. This opacity can breed distrust, especially when such AI systems are applied to high-stakes domains like public policy and governance that have direct impacts on citizens' lives. By providing clear explanations for how the AI arrives at its outputs, whether it is generated text, images or other content, emerging techniques in explainable AI (xAI) can help alleviate fears around black box algorithms making opaque decisions that impact citizens (de Bruijn et al., 2022; Leewis & Smit, 2023).

Moreover, Nigeria's substantial digital divides across rural–urban, socioeconomic and gender lines pose barriers to equitable access and inclusion for AI-driven civic engagement platforms. Therefore, by contextualising the possibilities of generative AI within Nigeria's democratic realities, the challenges of corruption, ethnic tensions, human rights considerations, digital inequalities and civil society's advocacy roles, a more grounded and holistic perspective can emerge. This context-specific framing illuminates not just the theoretical potential of AI, but pragmatic pathways for responsible implementation attuned to societal needs and risks. Ultimately, such nuanced analysis anchored in Nigeria's democratic milieu is crucial for developing strategies to harness generative AI as a force for inclusive, participatory governance rather than an amplifier of asymmetries and divisions.

5. Opportunities for generative AI in Nigerian e-government

5.1. Simplify conversation processes

Conversational agents and interactive guides powered by AI could indeed play a transformative role in simplifying complex policies and governance processes for citizens. These AI-powered virtual assistants, customised for local contexts, could serve as an accessible and user-friendly interface between citizens and e-government services (Guo et al., 2023). For instance, a citizen could interact with a conversational agent in the Nigerian Immigration Service to inquire about a specific policy or process about obtaining and renewal of an international passport. The agent, using its AI capabilities, could then provide a simplified explanation or guide the citizen through the process step-by-step. This could make it easier for citizens to understand and navigate complex governance processes. Moreover, these virtual assistants could also serve as a resource directory, answering citizen queries and directing them to relevant resources. Such applications of AI in e-government could make governance more comprehensible and user-friendly. By providing clear, accessible information and guidance, these technologies could help to demystify complex policies and processes, empowering citizens to engage more effectively with their government.

5.2. Cost effective means of communication

Generative AI tools indeed offer the potential to cost-effectively reach underserved populations, such as those in rural areas without internet access (Dev et al., 2023). Interactive voice response (IVR) systems, which can be accessed by phone, could provide key information and services in different languages to those who are disconnected from the digital world (Chui et al., 2023). These systems could use AI to generate responses to user queries, making them more interactive and user-friendly. Moreover, Nigeria with ethnic groups of over 250 with diverse languages can make use of this window by employing AI-generated content translated into local languages to further expand access. By providing information in a language that users are comfortable with, these tools can make e-government services more accessible and inclusive. This could be particularly beneficial in countries with diverse linguistic communities.

5.3. Increasing citizen awareness

Leveraging on generative AI could indeed play a significant role in increasing citizen awareness and adoption of e-government services (Symeonidis et al., 2023). AI virtual assistants powered by GPT-4, deployed on public service apps, could engage citizens in the digital spaces they already frequent. This approach brings the information directly to the citizens, rather than requiring them to seek out the information themselves. These

assistants could provide tailored, interactive explanations about various e-government services. By responding to individual queries and providing information in a conversational manner, these assistants could help overcome wariness and lack of understanding around existing platforms. They could demystify complex processes and make e-government services seem more approachable and user-friendly. Moreover, they could be programmed to provide information in local languages and dialects, further increasing their accessibility by considering local cultural contexts, making their interactions more relatable and effective.

6. Developing a comprehensive implementation and governance framework

To harness the potential of generative AI for enhancing civic engagement while mitigating associated risks, Nigeria must develop a comprehensive implementation and governance framework tailored to its unique context. This framework should be built through collaborative efforts involving diverse stakeholders, drawing from lessons learned globally while addressing local realities.

6.1. Stakeholder engagement

Engaging a wide range of stakeholders is crucial from the outset. This includes technology experts who can advise policy-makers on the capabilities and limitations of generative AI , to ensure alignment with national objectives, ethics boards to uphold moral principles, and perhaps most importantly, civil society groups and citizen representatives to voice end-user needs and concerns. Such inclusive consultation processes build legitimacy and public trust, which are critical ingredients for successful adoption of novel technologies in the civic sphere.

6.2. Legislative and regulatory mechanisms

Clear legislative and regulatory mechanisms governing public sector use of AI must be established. These should mandate algorithmic audits by independent bodies to detect and mitigate emerging biases or inaccuracies. Robust data privacy and security standards, adhering to global best practices while reflecting local cultural norms around information rights are imperative. Specific provisions dealing with data sovereignty, preventing misuse for surveillance or human rights violations given Nigeria's complex history should be prioritised.

6.3. Human-centric co-design

A human-centric, co-design approach involving extensive user research and feedback loops across Nigeria's diverse populace is vital. This means not just designing generative AI tools for citizens, but actively designing with representative citizens. Hands-on usability testing with rural, urban, literate and semi-literate user groups can uncover accessibility barriers, socio-cultural disconnects or interface friction points missed by technologists. Iterative improvements based on this feedback create AI-powered solutions attuned to how Nigerians communicate, consume information and navigate bureaucracies.

6.4. Digital enablement and literacy

No technological intervention, no matter how well-designed, can succeed without addressing digital divides. Nigeria must couple its generative AI roadmap with substantial investments in digital literacy programs, with a specific focus on underserved rural, low-income and female demographics. Building digital fluencies ranging from device usage to cybersecurity and online citizenship rights empowers citizens to meaningfully engage with AI-enabled services. Parallel investments in internet infrastructure, public digital access points and electrification are prerequisites.

6.5. Institutional capacity building

Adequate institutional capacity, through technical skill development and change management initiatives within the public sector workforce is essential. This ensures government agencies to effectively deploy, maintain and iteratively update AI systems aligned with policy objectives. Strategic partnerships with academia and industry could facilitate knowledge transfer and joint research for developing contextually relevant AI applications.

Nigeria can draw valuable lessons from the generative AI governance frameworks emerging across the globe. The European Union's proposed AI Act provides a comprehensive risk-based approach covering trustworthy AI principles like human oversight, robustness and transparency (Duberry, 2022). Similarly, India's initiatives like the National AI Strategy underscore stakeholder empowerment, skilling and ethical guardrails (Chatterjee, 2020). Singapore's pioneering Model AI Governance Framework is another example that details institutional vehicles for responsible AI deployment (Joo, 2023). Such exemplars provide useful policy templates for Nigeria to consider and localise.

Most importantly, developing a robust governance framework catalyses the positive impact of the generative AI as a democratising force for civic engagement within Nigerian e-governance. However, this transformative potential is contingent on inclusive multi-stakeholder involvement, meticulous human-centric design, unwavering prioritisation of ethics and public interests, and thoughtful navigation of socio-cultural complexities.

An adaptable, made-in-Nigeria framework balancing innovation with responsible steward-ship is crucial for harnessing generative AI as a citizen-empowering tool that bridges divides, boosts transparency and reinvigorates participatory democracy.

7. Conclusion

This paper explored opportunities and challenges associated with leveraging generative AI to boost civic participation within Nigeria's developing e-government landscape. Emerging generative technologies like ChatGPT demonstrate intriguing potential to make governance more interactive, accessible and engaging for citizens. Conversational interfaces could allow personalised explanation of complex policies, while virtual assis-tants provide new easy-to-use channels for the disconnected to engage with e-services. However, risks around bias, privacy, security and capability limitations must be navi-gated for successful implementation in the public sector. Further advances in AI will be required to enable truly open-ended dialogue needed for rich deliberative engagement. Additionally, Nigeria's substantial digital divides and erosion of public trust pose barri-ers to adoption. Targeted strategies focused on inclusion, accessibility, education and building institutional legitimacy will be critical to realise the promise of AI-enabled civic participation. Largely, generative AI merits cautious optimism as a tool for advanc-ing e-government, but one requiring good governance, human-centric design and responsible development attentive to risks. Further research and controlled pilots are needed to determine optimal applications and guardrails. If thoughtfully implemented and regulated, generative systems could open new possibilities for reimagining civic engagement and energising Nigeria's democracy in the digital age.

References

Abdulkareem, A. K. (2015). Challenges of E-Government Implementation in the Nigerian Public Service. *Journal of Creative Writing, 1*(4), 45–56.

Abdulkareem, A. K., Abdulkareem, Z. J., Ishola, A. A. & Akindele, I. T. (2022a). Does E-Government Impact E-Participation? The Influence of Trust in E-Government. *International Review of Public Administration, 27*(2), 91–110. Online: https://doi.org/10.1080/12294659.2022.2071540

Abdulkareem, A. K., Abdulkareem, Z. J., Ishola, A. A., Bello, M. L. & Oladimeji, K. A. (2022b). The Influence of Openness of Public Organizations and Social Media Use on E-Participation: The Mediating Effect of Trust in E-Government. *International Review of Public Administration, 27*(4), 281–296. Online: https://doi.org/10.1080/12294659.2022.2136054

Abdulkareem, A. K. & Ishola, A. A. (2016). E-government in Nigeria: Progress and Prospects. *Ilorin Journal of Administration and Development, 2*(1), 59–67.

Abdulkareem, A. K., Ishola, A. A. & Abdulkareem, Z. J. (2021). E-Government and Bureaucratic Corruption in Nigeria: Successes and Challenges. *Jurnal Studi Pemerintahan, 12*(1), 1–20. Online: https://doi.org/10.18196/jgp.121125

Abdulkareem, A. K. & Ramli, R. M. (2021). Does Digital Literacy Predict E-Government Performance an Extension of Delone and Mclean Information System Success Model. *Electronic Government, an International Journal, 17*(4), 466–493. Online: https://doi.org/10.1504/EG.2021.118103

Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A. & Lachana, Z. (2019, January 8–11). Benefits and Obstacles of Blockchain Applications in e-Government. *Proceedings of the 52nd Hawaii International Conference on System Sciences* (HICSS-52), Wailea, Hawaii, US.

Androutsopoulou, A., Karacapilidis, N., Loukis, E. & Charalabidis, Y. (2019). Transforming the Communication between Citizens and Government through AI-Guided Chatbots. *Government Information Quarterly, 36*(2), 358–367. Online: https://doi.org/10.1016/j.giq.2018.10.001

Androutsopoulou, A. S., Karacapilidis, N. I., Loukis, E. & Charalabidis, Y. K. (2021). Combining Technocrats' Expertise with Public Opinion through an Innovative E-Participation Platform. *LEEE Transactions on Emerging Topics in Computing, 9*(1), 174–187. Online: https://doi.org/10.1109/TETC.2018.2824022

Balaji, M. & Yuvaraj, N. (2019). Intelligent Chatbot Model to Enhance the Emotion Detection in Social Media Using Bi-Directional Recurrent Neural Network. *Journal of Physics: Conference Series, 1362.* Online: https://doi.org/10.1088/1742-6596/1362/1/012039

Baldauf, M. & Zimmermann, H.-D. (2020, July 19–24). Towards Conversational E-Government: An Experts' Perspective on Requirements and Opportunities of Voice-Based Citizen Services. *HCI in Business, Government and Organizations: 7th International Conference, HCIBGO 2020,* Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark.

Cantador, I., Viejo-Tardío, J., Cortés-Cediel, M. E. & Rodríguez Bolívar, M. P. (2021). A Chatbot for Searching and Exploring Open Data: Implementation and Evaluation in E-Government. *DG. O2021: The 22nd Annual International Conference on Digital Government Research* (pp. 168–179). Online: https://doi.org/10.1145/3463677.3463681

Chatterjee, S. (2020). AI Strategy of India: Policy Framework, Adoption Challenges and Actions for Government. *Transforming Government: People, Process and Policy, 14*(5), 757–775. Online: https://doi.org/10.1108/TG-05-2019-0031

Chohan, S. R. & Akhter, Z. H. (2021). Electronic Government Services Value Creation from Artificial Intelligence: AI-Based E-Government Services for Pakistan. *Electronic Government, 17*(3), 374–390. Online: https://doi.org/10.1504/EG.2021.116003

Chui, M., Hazan, E., Roberts, R., Singla, A. & Smaje, K. (2023, June 14). *The Economic Potential of Generative AI.* McKinsey Digital. Online: https://shorturl.at/lAIMT

De Bruijn, H., Warnier, M. & Janssen, M. (2022). The Perils and Pitfalls of Explainable AI: Strategies for Explaining Algorithmic Decision-Making. *Government Information Quarterly, 39*(2). Online: https://doi.org/10.1016/j.giq.2021.101666

Dev, S., Goyal, J., Tewari, D., Dave, S. & Prabhakaran, V. (2023). *Building Socio-culturally Inclusive Stereotype Resources with Community Engagement.* Online: https://doi.org/10.48550/arXiv.2307.10514

Duberry, J. (2022). *Artificial Intelligence and Democracy. Risks and Promises of AI-Mediated Citizen–Government Relations.* Edward Elgar Publishing.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., Carter, L. et al. (2023). Opinion Paper: "So What If ChatGPT Wrote It?" Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy. *International Journal of Information Management, 71.* Online: https://doi.org/10.1016/j.ijinfomgt.2023.102642

Guenduez, A. A. & Mettler, T. (2023). Strategically Constructed Narratives on Artificial Intelligence: What Stories Are Told in Governmental Artificial Intelligence Policies? *Government Information Quarterly, 40*(1). Online: https://doi.org/10.1016/j.giq.2022.101719

Guo, M., Zhang, X., Zhuang, Y., Chen, J., Wang, P. & Gao, Z. (2023). *Exploring the Intersection of Complex Aesthetics and Generative AI for Promoting Cultural Creativity in Rural China after the Post-Pandemic Era.* Online: https://doi.org/10.48550/arXiv.2309.02136

Joo, Y.-M. (2023). Developmentalist Smart Cities? The Cases of Singapore and Seoul. *International Journal of Urban Sciences, 27*(sup1), 164–182. Online: https://doi.org/10.1080/12265934.2021.1925143

Ju, J., Meng, Q., Sun, F., Liu, L. & Singh, S. (2023). Citizen Preferences and Government Chatbot Social Characteristics: Evidence from a Discrete Choice Experiment. *Government Information Quarterly, 40*(3). Online: https://doi.org/10.1016/j.giq.2022.101785

Leewis, S. & Smit, K. (2023, January 3–6). What Other Factors Might Impact Building Trust in Government Decisions Based on Decision Support Systems, Except for Transparency and Explainability? *56th Hawaii International Conference on System Sciences* (HICSS-56 2023), Maui, Hawaii.

Loukis, E., Saxena, S., Rizun, N., Maratsi, M. I., Ali, M. & Alexopoulos, C. (2023). ChatGPT Application vis-a-vis Open Government Data (OGD): Capabilities, Public Values, Issues and a Research Agenda. In I. Lindgren et al. (Eds.), *Electronic Government* (pp. 95–110). Springer, Cham. Online: https://doi.org/10.1007/978-3-031-41138-0_7

Mahapatra, R., Sharma, N., Trivedi, A. & Aman, C. (2012). Adding Interactive Interface to E-Government Systems Using AIML Based Chatterbots. *2012 CSI Sixth International Conference on Software Engineering* (CONSEG). Online: https://doi.org/10.1109/CONSEG.2012.6349510

National eGovernment Strategies (2019). *National eGovernment Strategies.* Online: https://shorturl.at/uxAMS

Ojeda, C. (2021). The Political Responses of Virtual Assistants. *Social Science Computer Review, 39*(5), 884–902. Online: https://doi.org/10.1177/0894439319886844

Omotoso, F. (2014). Public-service Ethics and Accountability for Effective Service Delivery in Nigeria. *Africa Today, 60*(3), 119–139. Online: https://doi.org/10.2979/africatoday.60.3.119

Oni, A. A. & Okunoye, A. O. (2019). Critical Success Factors in E-Democracy Implementation. In M. Khosrow-Pour (Ed.), *Advanced Methodologies and Technologies in Government and Society* (pp. 186–194). Information Science Reference. Online: https://doi.org/10.4018/978-1-5225-7661-7.ch016

Oyedele, S. O. (2015). The Nigerian Public Service and Service Delivery under Civil Rule. *Journal of Public Administration, Finance and Law, 7,* 33–43.

Seböck, W., Biron, B. & Lampoltshammer, T. J. (2023). Barriers to the Introduction of Artificial Intelligence to Support Communication Experts in Media and the Public Sector to Combat Fake News and Misinformation. In N. Edelmann, L. Danneels, A. S. Novak, P. Panagiotopoulos & I. Susha (Eds.), *Electronic Participation* (pp. 67–81). Springer. Online: https://doi.org/10.1007/978-3-031-41617-0_5

Shang, G., Low, S. P. & Lim, X. Y. V. (2023). Prospects, Drivers of and Barriers to Artificial Intelligence Adoption in Project Management. *Built Environment Project and Asset Management,* 13(5), 629–645. Online: http://dx.doi.org/10.1108/BEPAM-12-2022-0195

Smith, S. & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management, 23*(2), 23–32. Online: http://dx.doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4

Strauss, S. (2023). *Some Emerging Hypotheses about Using Generative AI in Public Sector Operations.* Online: https://dx.doi.org/10.2139/ssrn.4544943

Symeonidis, S., Samaras, S., Stentoumis, C., Plaum, A., Pacelli, M., Grivolla, J., Shekhawat, Y., Ferri, M., Diplaris, S. & Vrochidis, S. (2023). An Extended Reality System for Situation Awareness in Flood Management and Media Production Planning. *Electronics, 12*(12). Online: https://doi.org/10.3390/electronics12122569

Tisland, I., Sodefjed, M. L., Vassilakopoulou, P. & Pappas, I. O. (2022). The Role of Quality, Trust, and Empowerment in Explaining Satisfaction and Use of Chatbots in E-Government. In S. Papagiannidis, E. Alamanos, S. Gupta, Y. K. Dwivedi, M. Mäntymäki & I. O. Pappas (Eds.), *The Role of Digital Technologies in Shaping the Post-Pandemic World* (pp. 279–291). Springer. Online: https://doi.org/10.1007/978-3-031-15342-6_22

Ukiwo, U. (2006). *Creation of Local Government Areas and Ethnic Conflicts in Nigeria. The Case of Warri, Delta State.* Unpublished manuscript.

Valle-Cruz, D. & García-Contreras, R. (2023). Towards AI-driven Transformation and Smart Data Management: Emerging Technological Change in the Public Sector Value Chain. *Public Policy and Administration.* Online: https://doi.org/10.1177/09520767231188401

Vrabie, C. (2023). E-Government 3.0: An AI Model to Use for Enhanced Local Democracies. *Sustainability, 15*(12). Online: https://doi.org/10.3390/su15129572

Wirtz, B. W., Langer, P. F. & Fenner, C. (2021). Artificial Intelligence in the Public Sector – A Research Agenda. *International Journal of Public Administration, 44*(13), 1103–1128. Online: https://doi.org/10.1080/01900692.2021.1947319

Wirtz, B. W., Weyerer, J. C. & Kehl, I. (2022). Governance of Artificial Intelligence: A Risk and Guideline-based Integrative Framework. *Government Information Quarterly, 39*(4). Online: https://doi.org/10.1016/j.giq.2022.101685

Yang, L. & Wang, J. (2023). Factors Influencing Initial Public Acceptance of Integrating the ChatGPT-Type Model with Government Services. *Kybernetes.* Online: https://doi.org/10.1108/K-06-2023-1011

Yusuf, Y. A., Yusoff, K. Z. H. & Zengeni, K. T. (2018). The Implications of the Legislative Corrupt Practices on the Democratic Consolidation in the Nigeria's Fourth Republic. *Journal of Techno Social, 10*(1), 15–22. Online: https://doi.org/10.30880/jts.2018.10.01.002

Latvia's Ambiguous Attitude towards the Framework Convention for the Protection of National Minorities: Is Diversity a Threat?

Kiryl Kascian*

* Board Member, International Centre for Ethnic and Linguistic Diversity Studies, Prague, the Czech Republic, e-mail: kiryl.kascian@gmail.com

Abstract: On 22 February 2024, the Advisory Committee on the Framework Convention for the Protection of National Minorities published a critical opinion on Latvia within the framework of the fourth monitoring cycle. This text is centred on government comments as an important element of the standardised FCNM monitoring mechanisms provided by the Latvian Government during the four monitoring circles. This study identifies and assesses the key arguments and techniques employed by Latvia in this sectoral dialogue framework. It shows that the Latvian authorities view diversity as a threat to social cohesion, and their endeavours, inter alia, in the minority education domain, combine references to Latvia's traumatic historical experience, constitutional identity, and the margin of state discretion that camouflage the absence of political will to advance minority rights. Among other negative factors, this signals a dangerous path that could likely be followed by other states that are parties to this Convention.

Keywords: Latvia, national minorities, Framework Convention for the Protection of National Minorities, European Court of Human Rights, equality, constitutional identity

1. Introduction

On 22 February 2024, the Advisory Committee on the Framework Convention for the Protection of National Minorities (FCNM) published its fourth opinion on Latvia. In the Committee's view, the FCNM implementation level in Latvia "underwent a marked decline during the monitoring period", *inter alia,* because its "authorities further reinforced an exclusive narrative of Latvian national identity inextricably linked to the Latvian language" and the country's "public discourse does not always distinguish between the actions of the Russian Federation and the domestic concerns of persons belonging to the Russian national minority, which is highly diverse" (Fourth Opinion, 2024, p. 4). The Committee interprets this as undue restrictions that affect access to minority rights.

In turn, the Latvian government comments (2024, p. 4) underline that "the Advisory Committee does not understand or does not want to understand the historical situation of Latvia", delivering the recommendations that could lead to the reduction of Latvian language use and its apparent destruction in the long term. Specifically, a considerable part of the Government's comments is dedicated to the development of the argument about the negative consequences of the USSR's Russification policies for the ethnic and linguistic landscape of today's Latvia, which, in the view of Latvian authorities, justifies the country's minority policies.

In their comments, Latvian authorities underlined that education in minority languages in post-Soviet Latvia was inherited from "the segregated education system established during the [Soviet] occupation" (Government comments, 2024, p. 6). It is hard not to agree with those experts who amount this interpretation of the concept of segregation to "a novelty for the international protection of minority rights" (Dimitrovs, 2019). This interpretation dates back to the judgement of the Constitutional Court of 23 April 2019, in Case No. 2018-12-01[1] on minority schools and was subsequently repeated, for instance, in Case No. 2018-22-01[2] pronounced on 13 November 2019. This logic of the Latvian Constitutional Court could be described as "a judicial path to nowhere" because "all subsequent judgments of this court on minority education in Latvia will likely be based on the very same arguments" (Kascian, 2019). This leaves minority activists in Latvia with a very limited scope of arguments when they attempt to claim before the Constitutional Court the violation of minority rights arising from Latvia's domestic legislation and international legal instruments.

Another important element of the argumentation by Latvian authorities is their reference to the case law of the European Court of Human Rights (ECtHR), specifically to the recent cases of *Valiullina and others v. Latvia* and *Džibuti and others v. Latvia* related to minority education. Latvian authorities' logic is based on the clash between the recommandatory nature of the conclusions of the Venice Commission and the binding nature of the ECtHR decisions. While the "Advisory Committee refers extensively to the conclusions of the Venice Commission on the 2018 education reform", Latvia suggests addressing the above judgements since "the Court found no violation of the right to education and prohibition of discrimination in relation to the 2018 education reform in public, municipal and private education institutions" (Government comments, 2024, p. 6). This approach of the Latvian authorities creates two problems for minority education rights advocacy: the first one derives from the fact that the "Court agreed with the Latvian government that the existence of minority rights was the problem and not the violation of said minority rights" (Ganty & Kochenov, 2023). The second arises from the fact that the European Convention on Human Rights (ECHR) and the FCNM are two different legal instruments within the Council of Europe legislative framework, and the ECtHR's mandate is to interpret the former and not the latter treaty. Although

---

[1]   This case resulted from the 2018 education reform, which restricted the options for education in minority languages in public schools. The Court found that legislative amendments contested by a group of MPs complied with Latvia's Constitution and international agreements.

[2]   In this judgement, the Constitutional Court extended its conclusions from Case 2018-12-01 to the situation of private schools and thus restricted the options for education in minority languages there.

the texts of the ECHR and the FCNM have much in common, the very existence of the latter convention suggests that it addresses the specific needs of national minorities that by virtue of their belonging to a numerically inferior group need an additional protection explicitly formulated in a specific legal tool.

The above puzzle, involving Latvian authorities' argumentation and minority activists' capacities to successfully claim violations of their rights, suggests the goal of this article. It primarily focuses on the strategies and argumentation of Latvian authorities in dialogue within the FCNM framework – that is, on what Latvia communicates internationally. For many, this could be the reverse logic because the primary focus has shifted from the justified criticism of the Latvian authorities from international advisory bodies, such as the FCNM Advisory Committee, for the minority policies pursued by Riga. This implies the inclusion of diverse Latvian domestic contexts, including the country's history, ethno-linguistic landscape and politics, which affect the contents of the law and the argumentation of those who design it. The design of this study is as follows: it begins with an explanation of the relevant domestic contexts and designates the key arguments and techniques employed by the Latvian authorities in their communication within the FCNM framework and divided across three elements, followed by their critical assessment. Based on this, a conclusion is made, arguing that a more sophisticated approach towards criticism of Latvian authorities' argumentation could potentially offer a solution countering the current path to nowhere.

2. Latvian domestic contexts

Latvia is a small EU member state. Its features include the existence of a significant minority constituency and a traumatic historical experience during the 20th century described below in this section of the paper. These two features intersect when Latvia's minority policies are analysed, as they include elements of the country's history, constitutional identity, current ethnic and linguistic composition, domestic political configurations and minority policies. Thus, four aspects should be explained for a reader unfamiliar with Latvian realities before going into legal details.

First, Latvia achieved its independent statehood for the first time in history as a result of "an unprecedented international crisis" caused by the First World War, but failed to preserve its independence through the Second World War (Purs, 2012, pp. 47–48). This independence was interrupted by the Soviet occupation in 1940, and Latvia became a de facto part of the USSR for nearly five decades. Soviet policies have significantly transformed Latvia's society, which is heavily embedded in the country's constitutional doctrine and official discourse. Latvia restored its independence on 4 May 1990 and perceives itself "as the same state whose independence was unlawfully terminated in 1940" (Ziemele, 2020, p. 111).

Second, national minorities have always formed a considerable proportion of Latvia's population. However, postwar Latvia faced a significant influx of labour force from other parts of the Soviet Union. The following table shows the historical dynamic ethnic composition of Latvia's residents based on the three population censuses: the 1935 census

was the last conducted in prewar independent Latvia, the 1989 census was the last organised by Soviet authorities, and the 2021 census was the most recent.

Table 1.
Ethnic composition of Latvia's population in a historical perspective

	1935		1989		2021	
Ethnicity	**Number**	**%**	**Number**	**%**	**Number**	**%**
Latvians	1,472,612	75.50	1,387,757	52.04	1,187,891	62.74
Livonians	944	0.05	135	0.01	160	0.01
Russians	206,499	10.59	905,515	33.96	463,587	24.49
Belarusians	26,867	1.38	119,702	4.49	58,632	3.10
Ukrainians	1,844	0.09	92,101	3.45	42,282	2.23
Poles	48,949	2.51	60,416	2.27	37,203	1.97
Lithuanians	22,913	1.17	34,630	1.30	21,517	1.14
Jews	93,479	4.79	22,897	0.86	4,372	0.23
Germans	62,144	3.18	3,783	0.14	2,447	0.13
Other	14,251	0.74	39,631	1.48	75,132	3.96
Total	1,950,502	100.00	2,666,567	100.00	1,893,223	100.00

Note: The 1935 census data cover the interwar territory of Latvia, including territories of the Abrene/Pytalovo district, which were formally ceded to Russia in 1945. For section "Other" percentage was calculated by subtracting the sum of the shares of the ethnic groups specified in the table from 100%, which in some cases can result in an error margin of 0.01.
Source: National Statistical System of Latvia, s. a.; Salnītis & Skujenieks, 1937.

As the table reveals, by the collapse of the USSR, the proportion of ethnic Latvians in Latvia had decreased to just above half of the population, whereas the share of ethnic Russians had grown to roughly one-third. Latvian authorities consistently refer to these historical demographics in their arguments to emphasise the sui generis case of Latvia before various international institutions. This historicisation is also embedded in constitutional doctrine. For instance, the Constitutional Court in Case No. 2004-18-0106 (13 May 2005) emphasised that in the USSR, Latvia was not capable of controlling and designing incoming labour migration. Specifically, the court argued that "the Soviet immigrants were not integrated into the society of Latvia", and "a school system based on the segregation principle" was developed instead of liquidated prewar minority schools.

Third, ethnic issues have always been important elements of Latvia's political landscape. In Latvia, "the sense of an impending demographic catastrophe" when ethnic Latvians "would slip into minority status in their own homeland and eventually extinction" (Purs, 2012, p. 95) was one of the main causes for anti-Soviet protests. This cautious approach is linked with the emergence of the category of the so-called Latvia's "non-citizens" (Latvian: *nepilsoņi*), i.e. the former Soviet citizens who were not qualified to automatically obtain Latvian citizenship after the restoration of independence and who did not receive any other citizenship ever since. In ethnic terms, this category is almost entirely formed by people belonging to national minorities. As of the 2021 census, this

group comprised 190,522 persons or 10.06 percent of the country's residents, subject to a further decrease. In Latvia, its non-citizens are not entitled to elect and be elected. After the restoration of independence, "the central characteristic of the Latvian party system is the deep and continuing cleavage between ethnic Latvians and Russian-speakers" (Auers, 2013, p. 87). Typically, "a[n ethnic] Latvian voter chooses among [ethnic] Latvian candidates" (Kolstø & Tsilevich,[3] 1997, p. 389), and patterns of electoral behaviour of the minority constituency mirror this approach. On the one hand, today's Latvia has all the characteristics of democracy by ensuring equal rights to its citizens through participation in elections and other political activities. On the other hand, neither political group with predominant or overwhelming minority constituencies has so far been part of the government, and the potential votes of non-citizens (should they be granted citizenship or electoral rights) could strengthen their electoral results. As a result, the Latvian case is an illustration when the dominant ethnic group enjoys ownership over the state by making it "a tool for advancing their national security, demography, public space, culture and interests" (Smooha, 2002, p. 475).

Fourth, Latvia signed the FCNM on 11 May 1995, and ratified it on 6 June 2005 (Council of Europe, s. a.) with the declaration that the concept of minorities within the meaning of the convention applies solely to Latvia's citizens. More than ten years between signature and ratification illustrates the complexity of the issue for Latvian political elites. In practice, there were "no legal obstacles to [earlier] ratification, only political ones", because some politicians did not see it as an urgent matter, others appealed not to divide the society or connected ratification with the termination of the protests against the formation of a unified education system (Morris, 2005, p. 258). In other words, Latvia's relationship with the FCNM caused many emotions from the beginning.

3. Latvia's interpretation of the FCNM: Narratives and strategies

Country-specific monitoring of FCNM implementation envisages a standardised approach. Among other things, it includes state reports and government comments as documents produced by authorities through the FCNM monitoring mechanism. However, it is not uncommon that State Reports do not "reflect openly on problematic issues" or demonstrate "how the FCNM is implemented in practice" (Phillips, 2002, p. 2). In this regard, the focus on government comments would be more sophisticated, as they envisage the reaction of the authorities towards the main points of critics and frequently develop arguments that are particularly important to understand the position of a specific state. Referring to Latvia's comments on the Advisory Committee's fourth opinion described in the introduction, this section addresses the contents of Latvia's government comments on all four monitoring cycles. It is divided across three interconnected elements: the identity of the state, relations with international bodies and ECtHR case law.

---

[3] Elsewhere in the text, he is referred to as Boriss Cilevičs.

3.1. In the shadow of the Soviet past, or Latvia as an allegedly special case

The phrase about the Advisory Committee's unwillingness or reluctance to consider the Latvian historical past as the key to explaining the current minority issues from the government comments on the Fourth Opinion on Latvia is essential to understanding the shift in Latvia's official rhetoric. In all three previous circles, Latvia's government consistently emphasised the need to address historical contexts. However, they focused on it to a significantly lesser extent and used a more restrained language.

In its comments within the first monitoring circle, the Latvian Government addressed the issue in the introduction. It emphasises that evaluation of the FCNM implementation "from the point of view of Latvia's historic experience" needs to distinguish between the country's citizens and non-citizens and comply with "the fundamental principles of Latvia as an independent sovereign state" (Government comments, 2011, p. 2). Subsequently, it provides a moderate explanation of Latvia's citizenship policies after the restoration of independence. The comments from the second and third monitoring cycles essentially repeat this position, as they emphasise the need to consider Latvia's specifics, historical context and the doctrine of state continuity (Government comments, 2014, p. 2; Government comments, 2018, p. 4).

Hence, the comments to the Fourth Opinion form a qualitative change, as they contain an in-depth explanation of the ethnic demography in Latvia throughout the 20th century, with relevant figures and examples of Soviet Russification policies. Some provisions have clear patterns of securitisation in the context of the region's current situation. Specifically, Latvia articulates that "the Russian Federation's hybrid war and disinformation campaigns are also aimed at influencing the views of national minorities living in Latvia and that such actions pose a threat to both national security and the development of a cohesive society" (Government comments, 2024, p. 11). Indeed, Russia poses a threat to Latvia's national security, and Kremlin propaganda reaches its audience among some segments of Latvia's minority constituency. However, these hybrid threats would probably be less effective if Latvia's cohesive policies would better accommodate the country's ethnolinguistic diversity in the identity of the state and, eventually, apply different means to achieve social cohesion.

It seems reasonable to illustrate the logic of the country's cohesive policies through the interpretation of the 2012 referendum on the status of the Russian language as another official language in Latvia when 74.8 percent of Latvian citizens turned this initiative down. The Latvian Government argues that its result "confirms that both before and after the referendum, the responsible state institutions must do more, not less, to ensure that the will of the people – the use of the Latvian language – becomes a reality" (Government comments, 2024, p. 11). This argument is quite dubious because the referendum question did not even mention the Latvian language, and it would enjoy the status of Latvia's official language regardless of referendum outcomes. Yet, this argument by the Latvian Government complies with the identity of the state embodied in the *Satversme* (Constitution of Latvia) and judgements of the country's Constitutional Court. For instance, in its judgement in Case No. 2018-12-01, the Court recalls that the constitutional preamble (adopted on 19 June 2014, that is, after the referendum) contains

the values for an inclusive democratic society in Latvia, with the Latvian language as one of its core values and an inalienable element of the country's constitutional identity. In the court's view, it is an obligation of all permanent residents of Latvia to know the official language "on the level allowing full participation in the life of democratic society". Following this logic, it is merely an individual's duty to master the Latvian language to the required level based on the available options and not the state's task of ensuring the relevant education process of adequate quality.

On various occasions, many states, including Latvia, refer to their negative historical experiences, portray themselves as victims, and thus obtain certain political benefits. According to Boriss Cilevičs (2024): "Soviet annexation stopped Latvia's democratic development by force, and after the restoration of independence Latvia's political elites continue to adhere to the political logic rooted in interwar authoritarian Latvia under president Kārlis Ulmanis." This has a direct impact on minority policies. In Cilevičs's (2024) view, Latvian authorities perceive homogeneity as a norm and diversity as a threat; hence, equality could be achieved through elimination of these differences by minorities' assimilation for their own good. In practice, this stance of Latvian authorities places the state's goodwill as the key determinant of the scope and content of minority rights. This also contradicts the FCNM approach, which sees minority rights as an integral part of human rights.

3.2. International bodies and interpretation of sources

As mentioned earlier in the text, in its comments to the Fourth Opinion, the Latvian Government explicitly emphasised that the position of the Advisory Committee extensively relies on the conclusions of the Venice Commission which are "of a recommendatory nature" (Government comments, 2024, p. 6). However, a thorough look at the government comments from previous circles suggests that Latvian authorities had a different stance towards the assessments expressed by the Venice Commission at one instance. Specifically, in the first circle the Latvian Government extensively relied on its "Declaration on the consequences of state succession for the nationality of natural persons" (1996) to back its citizenship policies based on the principle of state continuity and justified by the need to recover "a political and legal identity which had been suppressed during the time of annexation" (Government comments, 2011, p. 4). A similar favourable position of the Parliamentary Assembly of the Council of Europe on this issue was mentioned as an additional argument.

A similar selectiveness can be observed in the practices of other Latvian institutions. For example, in Case 2019-20-03[4] (19 June 2020), the Constitutional Court in Case "dismissed quite easily the action letter by the Committee on the Elimination of Racial Discrimination and the letter of three UN Special Rapporteurs – as being based on their lack of comprehensive information" (Dimitrovs, 2020). These documents expressed

---

[4] In this case, the Constitutional Court found that restrictions on the use of minority languages in public and private kindergartens were consistent with the Constitution.

concerns regarding the new regulation of preschool education in the context of minority rights. However, the court saw them merely as an invitation to dialogue between Latvia and relevant international bodies.

The argument about the insufficient comprehensiveness of the information could be supplemented by the appeal to its accuracy, as demonstrated in the government comments on the Fourth Opinion on Latvia. While commenting on the linkage between Russia's aggression against Ukraine and the rights of Latvia's Russian minority, the government of Latvia regretted that the Advisory Committee "ignores the fact that by further strengthening the Russian language, the desire of a strong and self-sufficient minority to learn Latvian and integrate into Latvian society is being taken away" (Government comments, 2024, p. 4). Hence, the Advisory Committee's stance on the discrimination of this identifiable group of Latvia's society expressed in its Fourth Opinion was interpreted as false information distributed internationally.

Latvia is not unique in its selective attitude towards interpretations of certain events or policies by various international bodies who lack a mandate to issue legally binding decisions. This also confirms that "the FCNM remains a politically and legally weak instrument" (Morris, 2005, p. 251), particularly if the state is not interested in demonstrating its goodwill concerning specific contexts of minority issues.

3.3. ECtHR case law and FCNM contexts as seen by Latvian authorities

Specific references to the ECtHR case law appear in the Government comments (2024, p. 6) to the Fourth Opinion as an invitation for the Advisory Committee to "take [them] into account and refer to". They include three subject lines to be addressed here: minority education, rights of non-citizens and writing of personal names in the official documents issued by Latvia.

The first line includes the recent cases of *Valiullina and others v. Latvia* and *Džibuti and others v. Latvia,* and could be classified as a continuation of a quite frequent series of Latvian–Russian memory battles at the ECtHR (Muižnieks, 2011, pp. 219–220). The reason for this classification is the argumentation of the Latvian authorities to consider the context of the Soviet policies in Latvia and their impact on the current ethno-linguistic situation in the country. With no violations of the right to education and prohibition of discrimination within the context of the education reform found by the ECtHR, they serve as an argument for Latvian authorities to claim the correctness and consistency of their minority policies in education. It is based on three elements arising from the judgements. First, no obligation exists for the state to ensure education in the languages other than the official one. Second, the states have a significant margin of discretion on whether and how to ensure minority education. Third, "segregation" is the correct designation for the very fact of the education in minority languages, even though the need for it is backed by a considerable degree of demand by the country's national minorities. Hence, this logic puts the existence of the right to minority education solely to the state's good and eventual expediency.

These judgments became subjects of considerable criticism, which could probably best be wrapped up by an eloquent title of a piece by Ganty and Kochenov (2023) "Hijacking Human Rights to Enable Punishment by Association". Overall, Latvia's approach, as evidenced by the dialogue on FCNM implementation, is dangerous to the entire European minority rights system. As Aleksejs Dimitrovs (2024) emphasises, although scholars and practitioners currently proceed from an axiom that minority schools should be welcomed as a positive element for the preservation and development of ethnic identity, "Latvia, on the contrary, develops a narrative that the very existence of these schools amounts to segregation that poses danger to social unity".

The second line derives from the case *Savickis and others v. Latvia,* a case that links pension rights and citizenship factors. In its position, Latvia presented non-citizenship as a temporary instrument created for humanitarian purposes to prevent statelessness, with the option of obtaining either Latvian or other citizenship in the future. The Latvian Government emphasises that "non-citizenship status depends on non-citizens themselves should be given weight, as the legal framework allows them to naturalise", although it admits that many Latvia's residents with non-citizen status prefer not to do so (Government comments, 2024, p. 8). Hence, these facts prevent Latvia from accepting the Advisory Committee's proposal to extend minority rights to non-citizens. More importantly, the Latvian Government proposes that the Advisory Committee accepts the ECtHR's view on the naturalisation of citizens as a choice, as those "who decided not to naturalize in the country of residence are not entitled to non-discrimination" (Ganty & Kochenov, 2022; see also Nugraha, 2023).

In fact, *Savickis and others v. Latvia* stems from the situation in which the state did not recognise their employment beyond Latvia's borders during Soviet times that affected their pensions. Should they have been Latvian citizens, this problem would not have been an issue. Hypothetically, this situation could have affected Latvia's non-citizens irrespective of their ethnicity. As of 1 January 2024, there were 403 ethnic Latvians with a non-citizen status (Office of Citizenship and Migration Affairs, 2024, p. 4). Hence, this situation potentially extends beyond the minority context. Ganty and Kochenov (2022) further remind us that *Savickis and others v. Latvia* overruled *Andrejeva v. Latvia,* the case recalled by the Latvian Government in its comments during the second monitoring cycle. A comparison of these two cases deserves a separate analysis that goes beyond the thematic scope of this study. However, in 2014, the Latvian Government acknowledged that the issues pertinent to *Andrejeva v. Latvia* were successfully resolved. Meanwhile, it underlined that it would be groundless to extend the ECtHR conclusions from this case to the individuals "whose actual or legal situation differs considerably from that of Mrs Andrejeva irrespective of the fact that they currently reside in the territory of Latvia" (Government comments, 2014, p. 26).

The third line is based on the case of *Mentzen v. Latvia* and deals with the practice of writing personal names in the official documents of Latvia's citizens. After marriage to a German national, the applicant adopted her husband's surname Mentzen. However, in her new Latvian passport, her surname was inscribed as Mencena in compliance with the rules of the Latvian language to preserve the original pronunciation to the highest possible extent, with a special remark that confirmed that Mentzen was the original form

(Latvian: *oriģinālforma*). The reference to this case appears in the government comments on three occasions.

The first dates back to 2011, when Latvian authorities cited this case to emphasise that their restrictive practices have the legitimate aim "to protect the rights of other inhabitants of Latvia to use the Latvian language on all of Latvia's territory and to protect the democratic order" (Government comments, 2011, p. 31). They also stressed that state language, such as state territory and symbols, form core constitutional values. Hence, the decision of the Latvian authorities was presented as not violating an individual's right to decide how their personal names should be written. During the third monitoring cycle, Latvian authorities largely repeated these arguments and underlined the right of citizens to use the official language "also in communication with public authorities when sending or receiving information in that language" (Government comments, 2018, p. 21). The comments within the fourth monitoring cycle are quite concise, as Latvian authorities referenced this case to back their argument about the consistency of the practices of writing the personal names of Latvia's citizens in official documents with the country's international obligations (Government comments, 2024, p. 13). Later, they wrote that both the ECtHR and the Court of Justice of the European Union "have held that the presentation of personal names in Latvian has a legitimate aim" (Government comments, 2024, p. 26). The ECtHR practice is referenced in the case of *Mentzen v. Latvia,* whereas the CJEU approach is backed by the case *Malgožata Runevič-Vardyn and Łukasz Paweł Wardyn v. Vilniaus miesto savivaldybės administracija and Others.*

A reference to the case *Runevič-Vardyn and Wardyn* in the government comments works twofold for Latvia. On the one hand, as with any CJEU judgement, it serves as a precedent in subsequent cases with relevant effects on the judiciary and policy-making of other member states. On the other hand, it addresses Lithuania's situation. This southern neighbour of Latvia has also long been criticised for its practice of writing personal names in official documents. After the restoration of the independence of these two countries, Lithuania's approach in this domain, despite considerable similarities, has always been more liberal than that in Latvia, and after further liberalisation of Lithuanian legislation in January 2022 through the adoption of Law No. XIV-903, this discrepancy significantly increased (Kascian, 2023, pp. 73–86), but not in Latvia's favour. This legislative change provided relief for many Lithuanian citizens, both those who belong to national minorities and those of foreign spouses, irrespective of their ethnicity. Just before the vote on this law, Viktorija Čmilytė-Nielsen, speaker of the Lithuanian Parliament, stressed that this liberalisation is an important step that brings together human dignity, human rights and aspects of security (TVP Wilno, 2022). Therefore, Lithuania could serve as an example of a good, though not perfect, practice for Latvia in this domain, irrespective of what is written in the *Runevič-Vardyn and Wardyn* judgement.

Since Latvian authorities referred to the CJEU case law to back its arguments, the practices of this court should be discussed. In *Runevič-Vardyn and Wardyn,* the Luxembourg court referred to Article 4(2) TEU as a tool that protects the national identity of member states, including the protection of their official language. A more recent CJEU judgement in Case No. C-391/20 *Boriss Cilevičs and Others* concerning minority education in Latvia confirms the argument about the importance of the national identity of states pursuant

to Article 4(2) TEU. Overall, the outcomes of *Cilevičs and Others* case imply that Article 49 TFEU, as such, does not preclude the EU member states from limiting teaching in educational institutions solely to their official language provided that these measures are "justified on grounds related to the protection of its national identity, that is to say, that it is necessary and proportionate to the protection of the legitimate aim pursued". As Di Federico and Martinico (2023, p. 359) stress, "the identity clause – in its current formulation – was not intended to protect the linguistic diversity of the member states, which is in turn covered by other primary law provisions". Linked with the doctrine of state discretion, this logic of the CJEU contributes to the situation when EU law can be, and in fact, is used to hamper the scope of minority protection at the national level. Therefore, *Cilevičs and Others* can serve as further evidence of "the ineffectiveness of the use of national minority rights at the European level" (Krivcova, 2023).

4. Discussion and concluding remarks

An analysis of the public communication between Latvia and the Advisory Committee on the FCNM within the fourth monitoring cycle suggests that this legal instrument of the Council of Europe remains weak, both legally and politically. The decline in FCNM implementation in Latvia during this monitoring cycle is, in many ways, an extreme example. However, this situation has at least three implications: domestic contexts, case law of the relevant transnational courts, and the eventual patterning of Latvia's attitudes by other states that are parties to this convention.

As shown earlier, Latvia consistently demonstrates the approach when it is the state's goodwill, which determines the scope and content of minority rights. Hence, homogenisation is seen as a tool to achieve equality and social cohesion, and the existence of minority schools is perceived as segregation. It is a clearly opposite approach to that promoted by international bodies dealing with minority rights. This is in conjunction with references to the traumatic Soviet past, which, in the view of Latvia's authorities, makes the country a special case that should be considered to comprehensively evaluate minority policies and the implementation of relevant legal instruments. Finally, the case law developed by Latvia's Constitutional Court significantly contributed to this restrictive attitude. In various decisions on minority education, the Constitutional Court relied extensively on its own case law (Dimitrovs, 2020), and this path resembled a one-way road.

At the same time, the judgement in Case No. 2021-45-01[5] pronounced on 8 June 2023, contains a positive trend because it was the first example of case law by Latvia's Constitutional Court when the Satversme was interpreted in conjunction with the FCNM, and violation was found with regard to language and cultural minority education programs. More importantly, "the court put an end to the application of a populist approach, when the goal of protecting the state language justified any restrictions"

---

[5] This case deals with the use of minority languages in higher education. The Court found the contested norms of the Law on Higher Education Institutions inconsistent with the Constitution. Inter alia, the Court found that "universities have inherent academic freedom and the right to choose the language of instruction is part of this freedom" (Krivcova, 2023).

(Krivcova, 2023). This positive moment should not be exaggerated because it does not eliminate general trends. However, it demonstrates that there are still avenues to successfully challenge endeavours to undermine minority rights at the national level. Therefore, minority activists should not focus only on their argumentation on why specific documents or policies violate minority rights. In addition, they should pay meticulous attention to the analysis of the arguments used by relevant bodies and the judiciary to justify their endeavours aimed at undermining minority rights. Reliance on this analysis can contribute to more effective minority advocacy strategies.

The text also revealed that Latvian authorities effectively appeal to numerous ECtHR and CJEU case law as an additional argument to substantiate their position in communication with international bodies. This logic is reasonable, particularly when a legally binding reference with favourable content is measured vis-à-vis the critical one of a recommendatory nature. This demonstrates two interconnected systemic problems.

First, minority rights remain a niche topic that is frequently sidelined in favour of constitutional identity and protection of state language as an element thereof. Second, the example of Latvia demonstrates that judges at the ECtHR and the CJEU tend to see hampering minority rights as a lesser evil that characterises the corpus of the EU and the CoE legal acts, as interpreted by the relevant courts, as at least minority-unfriendly. For example, *Cilevičs and Others* shows that the CJEU "fail[ed] to elucidate the nature and intensity of the link between the relevant domestic measure and the identity element necessary to bring the situation within the realm of Article 4(2) TEU" (Di Federico & Martinico, 2023, p. 369). The same commentators also argue that in this specific case, the court opted not to address Article 22 of the Charter of Fundamental Rights of the European Union "to adequately balance the policy elaborated by the national legislator with (fundamental) minority rights" (Di Federico & Martinico, 2023, p. 369). As for the ECtHR, its attitude, demonstrated in the recent case law on Latvia discussed above, shows the path towards the toleration of abridging minority rights as a necessary and proportional step if this measure is justified by the need to protect state identity. Hence, the problem is not about the corpus of applicable law by the ECtHR and the CJEU, but about the attitudes towards their interpretation with a subsequent binding effect.

Finally, Latvia's stance towards FCNM implementation potentially shows a behavioural pattern for other states to fully or partially mirror it, appealing to extensive references to the specific situation caused by historical traumas or current threats and relying on a broad margin of state discretion. If chosen, it opens a potentially unbraked path to justify social homogeneity as a norm and diversity as a threat.

Acknowledgements

References

Auers, D. (2013). Latvia. In S. Berglund, J. Ekman, K. Deegan-Krause & T. Knutsen (Eds.), *The Handbook of Political Change in Eastern Europe* (pp. 85–123). Edward Elgar.

Council of Europe (s. a.). *Latvia, Country-specific Monitoring of the Implementation of the Framework Convention for the Protection of National Minorities.* Online: www.coe.int/en/web/minorities/latvia

Di Federico, G. & Martinico, G. (2023). Official Languages, National Identities and the Protection of Minorities: A Complex Legal Puzzle. Court of Justice (Grand Chamber) 7 September 2022, Case C-391/20, Boriss Cilevičs et al., ECLI:EU:C:2022:638. *European Constitutional Law Review, 19*(2), 346–370. Online: https://doi.org/10.1017/S157401962300010X

Dimitrovs, A. (2019, May 2). A Dangerous Precedent for Minority Rights: the Latvian Constitutional Court's Ruling on Minority Schools. *VerfassungsBlog.* Online: https://doi.org/10.17176/20190517-144117-0

Dimitrovs, A. (2020, June 23). Riga and Venice on a Collision Course: On the Controversial New Constitutional Court Decisions on Minority Languages in Latvia. *VerfassungsBlog.* Online: https://doi.org/10.17176/20200624-003808-0

Fourth Opinion (2024, February 22). Fourth Opinion on Latvia: Advisory Committee on the Framework Convention for the Protection of National Minorities. ACFC/OP/IV(2023)1. Online: https://rm.coe.int/4th-op-latvia-en/1680ae98f6

Ganty, S. & Kochenov, D. V. (2022, July 22). Citizenship Imposition Is the New Non-Discrimination Standard: ECtHR Blames the Victims in Savickis. *VerfassungsBlog.* Online: https://doi.org/10.17176/20220722-113542-0

Ganty, S. & Kochenov, D. V. (2023, November 23). Hijacking Human Rights to Enable Punishment by Association: Valiullina, Džibuti and Outlawing Minority Schooling in Latvia. *Strasbourg Observers.* Online: https://shorturl.at/hEP12

Government comments (2011, March 30). *Comments of the Government of Latvia on the First Opinion of the Advisory Committee on the implementation of the Framework Convention for the Protection of National Minorities by Latvia.* Online: https://rm.coe.int/1st-com-latvia-en/090000168008c94c

Government comments (2014, January 3). *Comments of the Government of Latvia on the Second Opinion of the Advisory Committee on the implementation of the Framework Convention for the Protection of National Minorities by Latvia.* Online: https://rm.coe.int/2nd-com-latvia-en/090000168008f51e

Government comments (2018, September 21). *Comments of the Government of Latvia on the Third Opinion of the Advisory Committee on the implementation of the Framework Convention for the Protection of National Minorities by Latvia.* Online: https://rm.coe.int/3rd-com-latvia-en/16808d91a6

Government comments (2024, February 19). *Comments of the Government of Latvia on the Fourth Opinion of the Advisory Committee on the implementation of the Framework Convention for the Protection of National Minorities by Latvia.* Online: https://rm.coe.int/4th-com-latvia-en/1680ae98f5

Kascian, K. (2019, October 3). Judicial Path to Nowhere? Challenging the Minority Education Reform before Latvia's Constitutional Court. *VerfassungsBlog.* Online: https://doi.org/10.17176/20191003-232709-0

Kascian, K. (2023). Evolution of Lithuania's Approach towards Writing of Personal Names in the Official Documents: On the Verge of Liberalisation? *Public Governance, Administration and Finances Law Review, 8*(2), 73–86. Online: https://doi.org/10.53116/pgaflr.6746

Kolstø, P. & Tsilevich, B. (1997). Patterns of Nation Building and Political Integration in a Bifurcated Postcommunist State: Ethnic Aspects of Parliamentary Elections in Latvia. *East European Politics and Societies, 11*(2), 366–391. Online: https://doi.org/10.1177/0888325497011002008

Krivcova, E. (2023, July 28). Language litigation in the field of higher education in the Constitutional Court of Latvia and the EU Court of Justice. *ICELDS.* Online: https://shorturl.at/bsA17

Muižnieks, N. (2011). Latvian–Russian Memory Battles at the European Court of Human Rights. In N. Muižnieks (Ed.), *The Geopolitics of History in Latvian–Russian Relations* (pp. 219–238). Academic Press of the University of Latvia.

Morris, H. M. (2005). The Non-Citizens of the EU. In D. J. Smith (Ed.), *The Baltic States and Their Region. New Europe or Old?* Vol. 3. On the Boundary of Two Worlds: Identity, Freedom, and Moral Imagination in the Baltics (pp. 251–273). Rodopi.

National Statistical System of Latvia (s. a.). Population by ethnicity at the beginning of year 1935–2023. Online: https://shorturl.at/nDEI5

Nugraha, I. Y. (2023). Protection of Constitutional Identity as a Legitimate Aim for Differential Treatment: ECtHR 9 June 2022, No. 49270/11, Savickis and Others v. Latvia. *European Constitutional Law Review, 19*(1), 141–162. Online: https://doi.org/10.1017/S1574019622000463

Office of Citizenship and Migration Affairs (2024, January 24). *Latvijas iedzīvotāju sadalījums pēc nacionālā sastāva un valstiskās piederības (Datums = 01.01.2024)* [Distribution of Latvia's population according to ethnic composition and nationality (Date = 01.01.2024)]. Online: www.pmlp.gov.lv/lv/media/11043/download

Phillips, A. (2002, September 1). FCNM: From Analysis to Action – Protecting minorities in Europe. *Minority Rights Group.* Online: https://shorturl.at/wCGQ3

Purs, A. (2012). *Baltic Facades. Estonia, Latvia and Lithuania Since 1945.* Reaktion Books.

Salnītis, V. & Skujenieks, M. (1937). *Ceturtā tautas skaitīšana Latvijā 1935. gadā. IV: Tautība* [Fourth Population Census in Latvia in 1935. IV: Nationality]. State Statistical Office. Online: https://shorturl.at/ahjHK

Smooha, S. (2002). The Model of Ethnic Democracy: Israel as a Jewish and Democratic State. *Nations and Nationalism, 8*(4), 475–503. Online: https://doi.org/10.1111/1469-8219.00062

TVP Wilno (2022, January 18). *V. Čmilytė-Nielsen o oryginalnej pisowni nazwisk: jest to kwestia godności ludzkiej* [V. Čmilytė-Nielsen on the Original Writing of Names: It Is a Question of Human Dignity]. Online: https://tinyurl.com/4a4pxfhy

Ziemele, I. (2020). A Non-Recognition Policy with Regards to the Occupation of Latvia. In A. Sprūds, V. Ščerbinskis & K. Bukovskis (Eds.), *The Centenary of Latvia's Foreign Affairs. Global Thought and Latvia* (pp. 100–116). Latvian Institute of International Affairs.

Personal communications

Cilevičs, B. (2024, March 5), former Latvian MP, former Chairperson of the Committee on Legal Affairs and Human Rights and the Committee on the Election of Judges to the European Court of Human Rights at the PACE.

Dimitrovs, A. (2024, February 11), legal advisor for the Greens/EFA Group in the European Parliament.

From Bonus to Onus:
Taiwan's Demographic Transition and Economic Development from 1950 to 2020

Kuang-Ho Yeh,* **Guihua Ni****

* PhD candidate in International Relations at the Institute of International Relations, Nanjing University, Nanjing, Jiangsu, China, e-mail: ry1207@gmail.com

** Postdoctoral Fellow at the School of Humanities and Social Science, the Chinese University of Hong Kong, Shenzhen, Guangdong, China, e-mail: niguihua@cuhk.edu.cn

Abstract: The driving force behind population change lies in fertility. Over the past 70 years, Taiwan has undergone a fertility transition, rapidly declining from a high peak of natural fertility levels to an ultralow rate. This transition released a substantial labour force and led to a significant shift in resource allocation, contributing to rapid economic development in the late 20th century. During the same period, Taiwan's population aging has progressed faster than that of most countries worldwide. The dependency ratio had a negative impact on economic development, making social security an important aspect of resource allocation. The changes in age structure have introduced the concepts of "demographic bonus" and "demographic onus". As a vibrant economy with a population of over 23 million, Taiwan has enjoyed the demographic bonus for more than a quarter of a century but is now facing the challenges of an aging society and declining fertility rates towards demographic onus. This article examines demographic transitions, economic performance and development in Taiwan from 1950 to 2020, elaborating on the definition, criteria, and quantitative delineation of the demographic bonus and demographic onus. It utilised population and economic statistics for a comparative analysis of the historical evolution, current situation, and prospects of the bonus and onus periods in Taiwan, providing a comprehensive narrative of its historical and empirical developments. Finally, the study underscores the complexity of balancing economic growth with demographic sustainability, emphasising the necessity for multiple policy adjustments to address the adverse effects of demographic transitions.

Keywords: demographic transition, demographic bonus, demographic onus, sub-replacement fertility, population aging

1. Introduction

During World War II, Taiwan, as a crucial colony of Japan, suffered intense Allied bombings, resulting in the destruction of over half of its industrial facilities and causing serious damage to economic productivity. After WWII, Taiwan was impacted by the Chinese Civil War, with the Kuomintang (KMT) government's high substantial military expenditures suppressing the island's economy from participating in investments. Simultaneously, to support the war effort, large amounts of resources were transported to mainland China, leading to shortages of essential goods and a sharp increase of inflation. In 1949, as the KMT regime retreated to Taiwan, over a million militants and civilians followed, causing a sudden surge in population that placed immense pressure on Taiwanese society. The economy also encountered huge challenges (Lin, 2018). In 1951, the GDP per capita of Taiwan was only $154, lower than the Philippines' $215 (adjusted to $922 using Maddison's purchasing power parity correction, still lower than Kenya in Africa with $947 at the same time). However, by the late 1980s, Taiwan had joined the ranks of the "Four Asian Tigers", with GDP per capita reaching $6,370 in 1988. By 2020, the number had reached $28,383, ranking 29th globally. Taiwanese economy had grown 184-fold over the span of 70 years, reflecting a remarkable development trajectory of rapid economic growth since the latter half of the 20th century.[1]

The transformations in Taiwan's population size and demographic structure are as remarkable as its rapid economic development. In the early 1950s, George W. Barclay predicted a population explosion for Taiwan. In his book *A Report on Taiwan's Population*, Barclay stated that with a population growth rate of 2.5%, the population of Taiwan will equal China's 450 million in 150 years (Barclay, 1954). However, the total population of Taiwan only increased from 7.98 million in 1950 to 23.57 million in 2020, far below Barclay's projection of an "explosive" increase. Regarding demographic structure, the decline in fertility rates began as early as the 1950s, which exhibited significant drops. The significant shift in fertility rates led American demographer Ronald Freedman to caution in 1986 that the Taiwanese government must carefully balance the positive and negative effects between population growth and economic development (Freedman, 1986). Additionally, the rapid decrease in mortality rates over the past decades has positioned Taiwan with the highest longevity levels globally. The process of population aging has been exceptionally swift, with the rate of aging second only to Japan in Asia.

In general, the impressive performance of Taiwan's economic growth since the 1950s has been attributed to the following macro-level factors (Mueller, 1977): 1. An ample labour supply, encompassing well-educated and skilled human resources; 2. Export-oriented industrial policies that led to the accumulation of substantial foreign exchange reserves and capital market; 3. Elevated savings rates and efficient capital allocation that facilitate investment in productive factors such as infrastructure; 4. Proficient application of advanced technologies introduced from developed countries.

These factors are closely connected to shifts in the demographic structure. Thus, this article aims to enrich the interdisciplinary understanding by examining the influence of

---

[1]   National Statistics, R.O.C. (Taiwan). Online: https://eng.stat.gov.tw/point.asp?index=1

demographic transition on Taiwan's economic performance since the latter half of the 20th century. It particularly emphasises the analysis of age structure transformation during different periods of economic development, illustrating the linkages between the demographic bonus process and economic variables. Moreover, by utilising the integral time frame of 1950 to 2020, it presents a thorough historical and empirical narrative of the overall demographic transition, highlighting the practical and real-world significance.

2. Literature review

To date, comprehensive research exploring the interrelationship between economic growth performance and demographic transition, particularly focusing on Taiwan, compared to the abundant individual accomplishments in these two fields, remains relatively limited. Regarding the former interdisciplinary achievements, the main research from Taiwanese scholars include the work of Yu and Wang (2009) who conducted an in-depth discussion of demographic qualitative change in Taiwan. They argued that during the agricultural phase of the economy, the relationship between population and economy was primarily manifested through the ownership and utilisation of land. In contrast, during the period when industry and commerce became the mainstream, the growth and movement of population depended on the level and the geographical location of development. Tsai (2004) argued that the development model led by Japan was built on export-oriented industrialisation under state guidance. Taiwan is considered the latecomer successfully replicating the Japanese model. The East Asian "flying geese" model of economic development drove waves of foreign investment flows. On the other hand, it caused a reverse migration of labour force, with Taiwan's population movement reflecting this regional trend. Li et al. (1990) drew on theories from history, economics and sociology, supplemented by demographic data of Taiwan, to examine population growth and demographic transition in modern Taiwan. They aim to clarify the relationship between population growth and economic development in Taiwan under various socio-economic conditions across different temporal and spatial contexts. Chen and Liu (2007) conducted research on socio-economic development as the underlying mechanism for population changes, integrating various socio-economic factors to explore their impact on age-specific fertility behaviours in Taiwan. Lin et al. (2010) predicted the future trends of labour force structure in Taiwan. Their findings indicate that Taiwan's future labour force is expected to decline, while the proportion of older workers will increase. This will lead to an increase in the average age of the labour force, and the labour dependency ratio will rise. Additionally, population aging will also lead to changes in the forms of wealth possession. Peng et al. (2009) explored the relationship between changes in population age structure and the slowing momentum of consumption growth in Taiwan, summarising the interaction effects on Taiwan's consumer market from three scenarios: changes in industrial structure, the M-shaped income distribution, and the trends of decreasing birth rates and aging population. Lin et al. (2015) constructed the model to examine the reciprocal feedback effects between population and macroeconomy, predicting Taiwan's population baseline from 2012 to 2060, estimating that by 2060, the total population in Taiwan

would be 14.78 million, approximately 8.14 million less than in 2012. Taking economic factors into account, they anticipate that rapid changes in population structure will lead to more severe child and elderly care issues. Huang et al. (2019) examined the impact of population and workforce aging on Taiwan using data from 1981–2017. Based on the empirical results, they argued that accounting for policy factors, increasing the supply of the eldercare workforce and foreign manpower contribute to countering the negative impact of an aging population on national economic growth.

Contributions from scholars in mainland China and overseas include the work of Jin and Dai (2012) pointed out that since Taiwan entered the aging society in 1993, the proportion of the elderly population has demonstrated rapid growth with an average annual increase of 22%. Based on the current aging rate, it is estimated that the proportion of the elderly population in Taiwan will double in 32 years, significantly surpassing France's 115 years. Chen and Yeh (2013) utilised population-related data of Taiwan from 1981–2011 to estimate the long-term relationship between population aging and industrial structure development. They found that population aging has a lag effect on the upgrading of the industrial structure and the development of the service sector. Over the long term, the trend of population aging has a gradually increasing positive impact on the advancement of the industrial structure. Mueller (1972) carried out Taiwanese household surveys, analysing a complex set of cost and benefit considerations that have an appreciable net effect on reproductive attitudes and behaviour, after socio-economic status and demographic characteristics have been considered. Tung (1984) used the econometric model with time series data from Taiwan to simulate the economic consequences of demographic change. The results suggest that in the short term, a slow-growing population yields substantially higher income per capita than does a fast-growing population, though in the long run, the fast-growing population generates slightly better economic performance. Deaton and Paxon (1999) analysed issues of household saving, growth and aging in Taiwan. The Taiwanese patterns of high-income growth declines in fertility and increases in life expectancy all have implications for life-cycle savings. Tsai et al. (2000) reviewed the theoretical hypothesis that changing survival rates affect households' decisions on savings. They found in the case of Taiwan that prolonged life expectancy helps raise the savings rate, while higher children's survival rates reduce it. Sanchez-Romero (2009) suggested that the contribution of demography to economic growth during the demographic transition in the case of Taiwan is given by the difference between the growth rate of the number of employees and the population, while the economic growth rate relies on productivity.

3. Demographic and socio-economic transitions in Taiwan from 1950 to 2020

The following figures illustrate distinct periods and the corresponding causal connections between demographic transition and socioeconomic transformation in Taiwan from 1950 to 2020: Figure 1 depicts the alterations in total fertility rate (TFR) spanning from 1950 to 2020, accentuating pivotal population events. Figure 2 exhibits the fluctuations in GDP growth rate over the same period.

3.1. Transformation in fertility rates and economic growth from 1950 to 2020

Due to the post-war baby boom, the fertility rate in Taiwan underwent changes similar to those in Western countries. The average total fertility rate for Taiwanese women of childbearing age peaked at 7 children in the early 1950s. By the 1960s, it had decreased to 5 following the introduction of oral contraceptives and the promotion of family planning. In the 1970s, with the increased participation of women in the workforce, the number of children being born decreased even more rapidly. By 1983, the total fertility rate had dropped to the replacement level of 2.1, where the total population remains constant over generations.[2] The total fertility rate decreased by 70% over the 30-year period from 1953 to 1983.
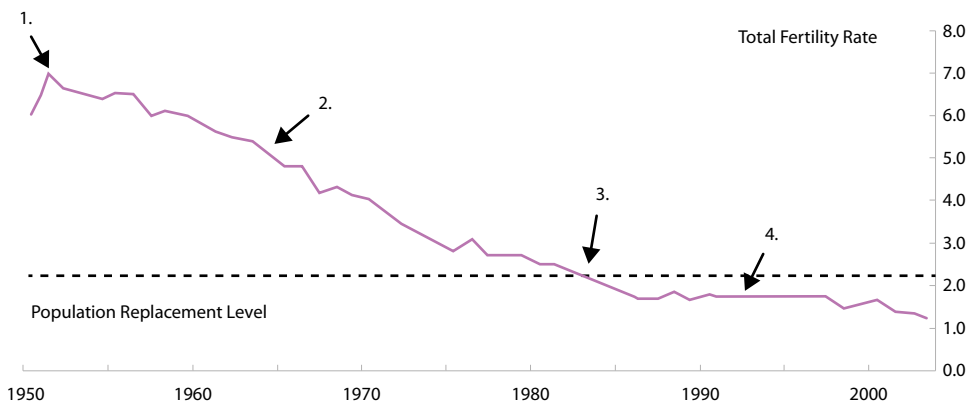

Figure 1.
Taiwan total fertility rate trend
Note: Historical traits of the total fertility rate trend curve: 1. Post-war baby boom in the early 1950s; 2. Comprehensive family planning launched in 1964; 3. Female labour force participation rate exceeds 40% in 1983; 4. Open up Taiwan to Mainland China spouses in 1992.
Source: Ministry of the Interior (Taiwan).

Mueller (1977) argued that the trend of rising and then falling fertility rates in Taiwan during the 1950s resulted in an early manifestation of growth in the labour force. The decline in fertility rates led to the growth rate of labour force faster than the overall population, providing a significant driving force for economic development through the sufficiency of labour supply. This trend also suppressed wage growth, as the abundant labour availability kept wages relatively low. The sustained low wage levels became the critical factor in the early economic growth of Taiwan from the 1950s to the 1970s. These lower wage levels shaped the competitiveness of the Island's export sector. The expansion of capital input in economy stemmed from the surplus generated by export

---

2   Social Indicators Statistics. Ministry of the Interior (Taiwan), 2004. Online: www.stat.gov.tw/public/data/dgbas03/bs2/si/93%E8%AD%B0%E9%A1%8C%E5%B0%88%E8%BC%89.pdf

trade, which, in turn, raised consumer demand and social welfare levels. The continuous decline in fertility rates further reduced the dependency burden on the labour force. Besides fostering the high savings rates required for capital input, this decline also contributed to the control of wage inflationary pressures for industrial sectors. Furthermore, personal financial allocation shifted significantly away from family expenses related to raising children, accelerating the accumulation of capital and laying a solid foundation for the rapid economic growth of the following decades.

However, in the 1990s, Taiwanese authorities recognised the emerging adverse effects of the declining population trend, that the demographic policy goal was adjusted from "mitigating" population growth to "maintaining reasonable population growth". With the increase in cross-border marriages due to globalisation, the decline in fertility rates slowed slightly in the early 2000s, which remained below 1.5 births per woman. Meanwhile, economic growth decelerated after the 2000s, with an average growth rate ranging between 1% to 3%. The economic structure, overly reliant on the technology of original equipment manufacturing (OEM), made the economy highly susceptible to fluctuations in the global market. In 2001, impacted by the Dot-com bubble, the Taiwanese economy contracted by −1.4%, marking the first negative growth since 1947. The unemployment rates concurrently reached an all-time high. In 2009, under the shadow of the global financial crisis, another low point of −1.61% growth emerged. The total fertility rates for both years also began a new downward trend after remaining stable or slightly increasing in previous periods.[3]
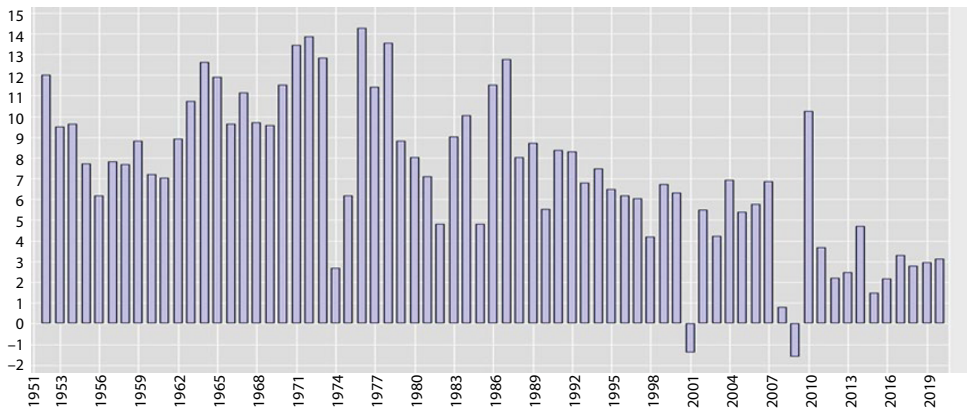

Figure 2.
Taiwan annual economic growth rate bar chart
Source: National Statistics, R.O.C. (Taiwan).

Since the 1990s, the phenomenon of stagnant real incomes has significantly impacted demographic transitions in Taiwan. The International Labour Organization (ILO) highlights common factors contributing to the decline in wage income worldwide:

---

[3]   Population Projections for the R.O.C. (Taiwan). National Development Council. Online: https://pop-proj.ndc.gov.tw/dataSearch2.aspx?r=2&uid=2104&pid=59

technological changes, the globalisation of trade and cross-border investments, the movement of financial capital, and institutional constraints within local labour markets. These factors explain the wage stagnation in Taiwan over the past two decades. Being a highly open small-scale economy, Taiwan has inevitably experienced the effects of globalisation. The economic magnetic effect emanating from the nearby market of mainland China exacerbates this situation, as the shared culture and language facilitate the complete transplanting of Taiwanese manufacturing chains. Wage stagnation in Taiwan is more severe compared to other economies. In 2001, the substantial wages in Taiwan and South Korea were nearly identical ($1,136.44 and $1,285.14). However, by 2020, the former was still hovering around $1,400, while the latter had surged to $3,000 (Huang et al., 2014).

In recent years, the intense competition between the US and China in the realms of geopolitics and trade has profoundly impacted the Asian high-tech industrial chain. Taiwan's tech sector, especially a few semiconductor giants, has boomed from this background (Chiang, 2023). However, the rapid expansion of chip-related portions such as electronic components, and the corresponding growth in exports have bolstered impressive nominal GDP figures but masked the real income challenges faced by the majority of the workforce on the island. Behind the phenomenon of TSMC as a single company accounting for nearly one-third of the value of the Taiwanese stock market, the actual situation of consumption expenditure, which reflects the income levels of ordinary Taiwanese people, has not met expectations, exposing the reality of an unbalanced overall economic structure (Hale, 2021). Wage rigidity further worsens the decline in fertility rates. After remaining at an extremely low level of 1 to 1.2 for a long time, in 2020, the number of deaths exceeded the number of newborns for the first time, officially pushing Taiwan into the "death cross" of negative population growth. In the CIA's 2021 World Factbook report, the predicted fertility rate for Taiwan was 1.07, ranking last among 227 political entities worldwide.[4]

3.2. Evolution of mortality rates from 1950 to 2020 and the establishment of the social security system

With the continuous decline in fertility rates, the mortality rate is also showing a dramatic downward trend. Between 1950 and 2000, the average life expectancy at birth in Taiwan increased from 55.3 years to 76.5 years. By the year 2020, life expectancy at birth had risen to 78.1 years for males and 84.8 years for females, marking it one of the places with the longest lifespan in the world. Figure 3 illustrates the long-term trend in life expectancy at birth for the population of Taiwan from 1950 to 2020. The rise in average age implies that advancements in medical care have contributed to enhancing the survival rate of the elderly. Beyond the supply and demand of medical services, the most effective way to cope with aging is to proactively plan for post-retirement needs.

---

[4] The World Factbook 2021–2022. Central Intelligence Agency, 2021. Online: www.cia.gov/the-world-factbook/field/total-fertility-rate/country-comparison

With these considerations, Taiwanese authorities have promoted the National Health Insurance (NHI), National Pension Insurance, and the long-term care insurance progressively since the mid-1990s. This endeavour has constructed a comprehensive social security system encompassing medical, socio-economic and caregiving dimensions.
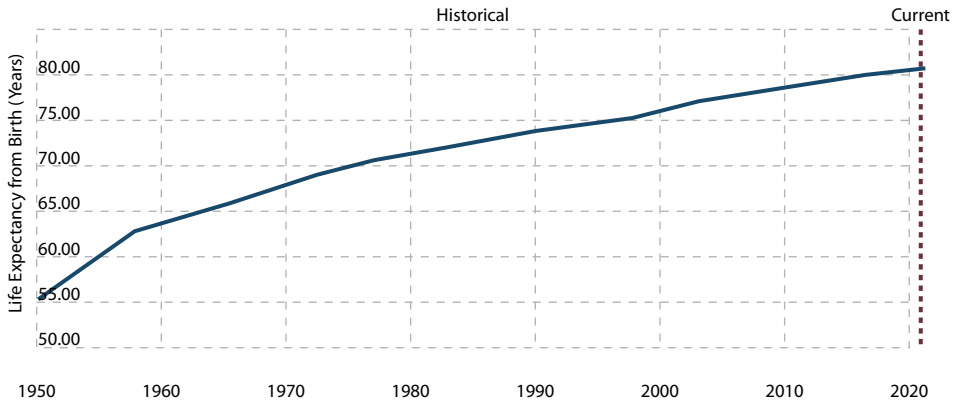

Figure 3.
Taiwan population life expectancy trend
Source: Taiwan Life Expectancy 1950–2024 [Data set], Macrotrends.net.
Online: www.macrotrends.net/countries/TWN/taiwan/life-expectancy

The National Health Insurance (NHI) implemented in 1995 provides health coverage for all residents across the island through mandatory medical insurance. The NHI contributes to extending the average life expectancy, particularly by reducing occurrences of medical avoidable mortality. A decade after its implementation, life expectancy increased by 2.6 years for males and 3.0 years for females, surpassing the increases observed prior to its implementation (1.4 and 2.3 years respectively). The NHI has also enhanced the equity of medical care for the vulnerable groups. Empirical evidence indicates that after the introduction of the NHI, the utilisation rates for outpatient and inpatient services among elderly individuals lacking other health insurance increased by 27.97% and 12.5%, which is in stark contrast to the much lower increase rates of 13.34% and 1.69% among the well-insured elderly. In 2008, Taiwan began implementing the National Pension Insurance to ensure individuals aged 25 to 65 who had not participated in other social insurance programs would maintain a basic living standard in their old age, thus safeguarding the economic security of the elderly population. From 1950 to 2020, the proportion of social security system expenditures in the public finance sector increased from 0.09% to 25.2%, marking a significant progress.[5]

Figure 4 depicts Taiwan's trajectory toward becoming an aging society in 1993, progressing to an aged society in 2018, and anticipated to evolve into a super aged society

---

[5]   The data of 1950 is in the Central Government Expenditure Final Accounts (1950). The data of 2020 can be found at the Analysis of Central Government Total Budget Expenditure (2020). National Statistics, R.O.C. (Taiwan).

by 2025, driven by a steep decline in fertility and mortality rates. The percentage of the population aged 65 and above surged from approximately 2% in 1950 to 16% in 2020, while the proportion of those aged 0 to 14 decreased from 40% to 12.5% during the same period. The aging index (the ratio of the elderly population to the youth population) rose remarkably from 5 to 128 over the course of 70 years.
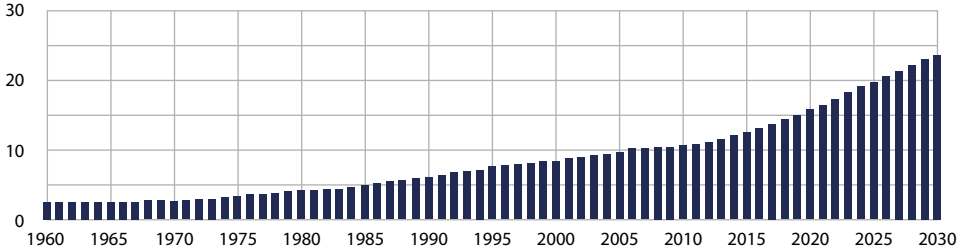
Figure 4.
Taiwan elderly population percentage trend
Source: National Development Council (Taiwan).

The total dependency ratio in Taiwan displayed a zigzag pattern from 1950 to 2020 (Figure 5). In the 1950s and 1960s, a substantial increase in the young population due to the baby boom resulted in the total dependency ratio peaking at 94.05 in 1962. Subsequently, it began to decrease steeply with the decline in fertility rates, reaching 34.74 by 2013. The continuous growth of the elderly population began to exert a dominant influence on the total dependency ratio at the same time. After 2013, the total dependency ratio started to rise again, and the child dependency ratio and the old-age dependency ratio intersected in 2017. From then on, the old-age dependency ratio became the determining factor of the total dependency ratio.
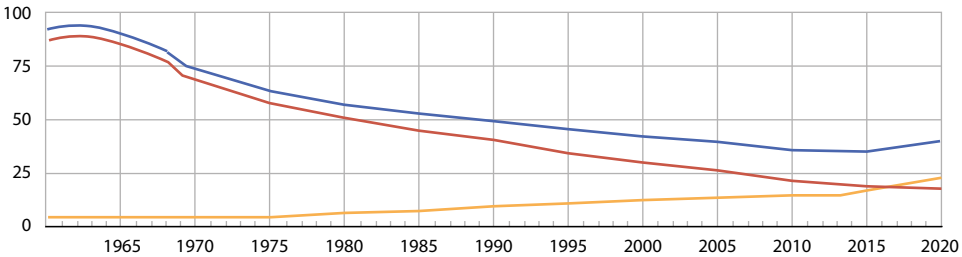
Figure 5.
Total (blue curve), youth (red) and elderly (orange) dependency ratio trend
Note: The child dependency ratio refers to the number of youth population supported by every hundred working-age population, while the old-age dependency ratio refers to the number of the elderly supported by the same population group.
Source: National Development Council (Taiwan).

4. "Demographic bonus" and "demographic onus": Macro-level assessment of the impact of demographic transition on economic development

Taiwan completed the demographic transition from high birth and death rates to low rates after 1983. Amid the slowdown in population growth, there was an expansion of the workforce, leading to a greater share of economic resources transmitted toward it. The shift reaped economic benefits brought about by a process spanning several decades from the mid-1960s (Chang & Lee, 2001). This article adopts a macro-level assessment approach, utilising historical data and quantitative methods to evaluate the impact of demographic transition phases on Taiwan's economy. It integrates a comparative analysis of different demographic stages and their respective economic impacts, thereby providing the perspective on the relationship between population dynamics and economic development.

"Demographic Bonus" interprets the time period when the age structure of the population enters a "harvest" phase, and a larger proportion of the labour force population plays a catalytic role in economic growth. According to the basic quantitative definition by the United Nations Population Fund (UNFPA), demographic bonus refers to the working-age population (ages 15–64) accounting for more than 66.7% of the total population, as the dependency ratio being lower than 50%. Meanwhile, the "demographic window" (UNFPA, 2010) signaling the entrance into the period of demographic bonus opens. Demographic bonus and its reverse function of "Demographic Onus"– the sustained population decline during the demographic bonus phase ultimately results in the shrunk working-age population bearing a significant burden of the social security and welfare costs for the larger non-working population, constitute the entire process and the overarching theory of "demographic dividend". The theory originally proposed by David E. Bloom and Jeffrey G. Williamson (1998), is based on changes in the proportions of population within the three age groups, reflecting the population structure and labour force required for economic development. Bloom and Williamson argued that a significant portion of the economic growth in the "Four Asian Tigers" during the 1960s to 1990s could be attributed to the transitions of demographic bonus. Generally, during the transition to low fertility and mortality rates, the natural increase in a country's labour force will create the so-called "demographic window". In this period, the dependency ratio will be low, and the mature cohort of the labour force has the capability to enhance the country's economic prosperity (Misra, 2015).

The demographic bonus is distributed through various interconnected mechanisms that can shape the overall circulation toward final economic growth, as depicted in Figure 6. In the context of demographic transition, the population structure shifts towards a larger proportion of the working-age population, which increases as the dependent population decreases due to policy intervention. Consequently, three feedback effects of the demographic bonus emerge: a release in labour supply, an increase in savings, and an improvement in the quality of human capital (Bloom et al., 2003). Firstly, the increased labour supply helps suppress wage costs, enhancing industrial competitiveness. The reduced

caregiving demands free up the labour force, especially among women, further augmenting the labour supply. Secondly, the change in population structure leads to a decrease in dependency expenditures. Since the consumption of the dependent population generally exceeds their production, the increased working-age population is motivated to save for their future retirement owing to the longer life expectancy. This raises the savings rate, thereby promoting domestic investment and contributing to the nation's social and financial growth. Lastly, the trend of the population structure shift is favourable for national, corporate and familial investments in human capital. The outcome of investing in one's own and the next generation's education and professional training is the substantial enhancement of economic productivity (Chen, 2016).

After amassing nearly four decades of demographic development momentum, Taiwan entered the demographic window in 1990, as the age structure of the population transitioned into the demographic bonus. Nevertheless, entering the 21st century, economic growth has shown a decline compared to the past, suggesting that the demographic bonus is gradually diminishing. This implies that the Taiwanese economy is on the verge of transitioning from a stage that reaps benefits from the demographic bonus to a phase that bears the burden of another continuous transition, which is referred to as the negative dividend stage of demographic onus. The following integrates and argues for the complete theory of demographic dividend, combining the development cases of Taiwan with different perspectives of representative scholars.
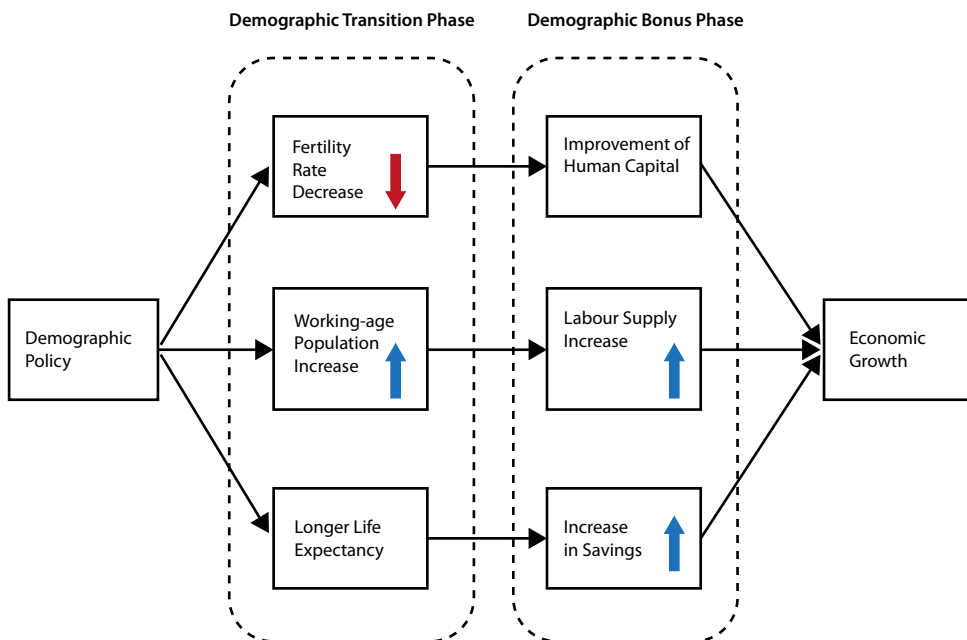

Figure 6.
The mechanism of demographic bonus loop
Source: Compiled by the authors.

4.1. Demographic bonus and economic development

Table 1 presents a combination of Taiwan's labour force participation rate, dependency ratio, and economic growth rate from 1990 to 2020, following the onset of the demographic bonus phase. The objective is to assess the impact of the declining fertility rate on economic development throughout the entire time span. The five-year average value (calculated as 6 years for 1990–1995) dilutes the impacts of individual years (2001, 2009, 2010) with extreme fluctuations in economic performance. The outcomes depicted in Table 1 reveal that Taiwan encountered a decline in economic growth after 2000, which did not seem to reflect the apparent positive impact of the demographic bonus on economic development. However, as mentioned earlier, the decline in Taiwan's economic growth rate indeed reflects the economy entering a transitional phase, influenced by multiple exogenous variables. At this juncture, the phenomenon of the demographic bonus is better interpreted as a "brake pad" effect exerted by demographic factors during economic recessions.

Table 1.
Labour force participation rate, dependency ratio and economic growth rate from 1990 to 2020

	Labour Force Participation Rate (%)	Dependency Ratio (%)	Economic Growth Rate (%)
1990–1995	67.64	47.87	7.17
1996–2000	69.70	43.48	5.89
2001–2005	70.93	40.99	4.13
2006–2010	72.68	37.61	4.41
2011–2015	74.07	35.01	2.91
2016–2020	72.46	38.02	2.87

Source: Ministry of Labour (Taiwan).

On the other hand, Ogawa et al. (2005), Wang and Mason (2006) define the demographic bonus as the period during which the growth rate of GDP per capita for the entire population exceeds the growth rate of GDP per worker employed. By broadening the concept of demographic bonus from a simplified change in age structure to a connection with economy, it highlights the core impetus of demographic bonus – the contribution to overall societal output resulting from the changes in the labour force structure. In contrast, the demographic onus exhibits a reverse pattern.

In accordance with the demographic bonus definition of Table 1, Table 2 calculates the five-year statistics for the growth rate of GDP per capita and the growth rate of GDP per worker starting from 1990. It is evident that in the initial five intervals from 1990 to 2015, the growth rate of GDP per capita exceeded that of GDP per worker. The results for output per capita and output per worker validate that the demographic bonus's impact on economic growth remained consistently active between 1990 and 2015. However, starting in 2016, the growth rate of GDP per capita fell below that of GDP per worker,

marking the inflection point. The underlying reason for this shift is that the labour force began to decline during this period (−1.3%), while the total population continued to rise. Consequently, the driving force of labour output contributing to the overall societal output significantly weakened.

Table 2.

GDP per capita, GDP per worker and the periodic growth rates in Taiwan from 1990 to 2020

	GDP (millions of USD)	GDP Per Capita (1)	GDP Per Worker (2)	Total Population (per thousand)	Total Labour Force (per thousand)	Growth Rate of (1)	Growth Rate of (2)
1990–1995	224,435	10,768	15,882	20,890	14,131	N/A	N/A
1996–2000	302,053	13,839	19,774	21,913	15,275	28.5	24.5
2001–2005	329,006	14,584	20,526	22,598	16,029	5.4	3.8
2006–2010	408,858	17,780	24,425	23,031	16,739	21.9	19.0
2011–2015	512,451	21,958	29,606	23,368	17,309	23.5	21.2
2016–2020	604,835	25,664	35,410	23,573	17,081	16.9	19.6

Note: The gray highlighted cells indicate the stages where the growth rate of GDP per capita was lower than that of GDP per worker.

Source: National Statistics, R.O.C. (Taiwan).

4.2. Degree of contribution of the demographic bonus to Taiwan's economic development

Chen Youhua (2008) formulated the model to calculate the quantitative contribution rate of the demographic bonus to economic growth as follows:

$$\text{GDP}_t^s = \frac{\text{GDP}_t}{\text{L}_t} \times \frac{\text{L}_s}{\text{P}_s} \times \text{P}_t (1)$$

GDP contribution rate of demographic transitional factors $= \dfrac{\text{GDP}_t - \text{GDP}_t^s}{\text{GDP}_t} \times 100\%$ (2)

In Formula (1), L and P represent the labour force and total population respectively. GDP_t, Lt, and Pt are values for the statistical year, while L_s and P_s are the labour force and total population to the reference population. GDP_t is the actual GDP for year t under the influence of demographic transition, while GDPs t represents the theoretical GDP for year t excluding the demographic impact. The contribution rate of demographic transitions to GDP is illustrated in Formula (2). The positive rate signifies the demographic bonus phase, while the negative rate indicates the demographic onus stage.

Table 3 illustrates the actual contribution of demographic transition to GDP growth between 1990 and 2020. Nearly 3% of GDP growth in the years 1996–2000 was attributed to the demographic bonus. However, during the years 2016–2020, the contribution rate turned negative, suggesting that the demographic bonus was approaching its end. This aligns with the economic impact of a declining labour force, as inferred from Table 2. It is confirmed that after going through different quantitative models, international scholars converge in their deduction processes regarding the relative change in the labour force population as the core variable in the demographic bonus loop. Such theoretical consistency reinforces the applicability of demographic bonus in explaining its impact on the economic aspect.

The following further deduces an analytical hypothesis based on the descriptive statistical verification of the existing theories mentioned above: GDP＝F(W). According to the data series of five-year statistics in Table 2, GDP represents the per capita output for different time periods, while W denotes the output level of the labour force at the same period. The empirical model is as follows: $\ln GDP = \alpha_0 + \alpha_1 \ln W$. When regression analysis was conducted using data from the period of demographic bonus from 1990 to 2015, it yielded the results: $\ln GDP = -1.696 + 1.13 \ln W$, with the P-value less than 0.05, indicating statistical significance. Additionally, $R^2 = 0.9993$, Adj-$R^2 = 0.9990$, indicating a proper goodness of fit of the model. The coefficient of the study variable is 1.13, indicating a positive correlation with the explained variable, and as the coefficient is greater than 1, it suggests a multiplier effect during the demographic bonus period driving the economy. However, when data from the period of demographic onus starting from 2016 are included, the coefficient decreases to 1.06, indicating a decline in the driving effect.

Table 3.
Contribution of demographic bonus to economic growth in Taiwan

	GDPt (millions of USD)	GDPst (millions of USD)	Contribution Rate of Demographic Bonus (%)	Pt (per thousand)	Lt (per thousand)	Ls/Ps	Pt/Lt
1985–1989	105,193	N/A	N/A	19,732	13,023	N/A	N/A
1990–1995	224,435	219,228	2.3	20,890	14,131	0.66	1.48
1996–2000	302,053	293,716	2.8	21,913	15,275	0.68	1.43
2001–2005	329,006	324,729	1.3	22,598	16,029	0.70	1.41
2006–2010	408,858	400,599	2	23,031	16,739	0.71	1.38
2011–2015	512,451	505,020	1.5	23,368	17,309	0.73	1.35
2016–2020	604,835	617,658	−2.1	23,573	17,081	0.74	1.38

Note: The gray highlighted cells indicate the declining trend in the labour force, and the negative contribution rate to GDP growth (−2.1%).

Source: National Statistics, R.O.C. (Taiwan).

4.3. The arrival of the demographic onus

The formation and persistence of the demographic bonus have provided a certain degree of support for Taiwan's economic development. The decline in the young population has led to an increased proportion of the labour force, thus extending the demographic bonus. However, the accelerating growth of the elderly population has consistently outpaced other age groups, making population aging the primary factor driving the end of the bonus period. Notably, the labour force that fuelled economic development during its peak began to retire after the 2010s, leading to widening gaps between variables. Estimated according to the UNFPA standard, Taiwan is projected to transition from the demographic bonus to the demographic onus stage by 2027. Based on calculations using the academic definitions, this article concludes that Taiwan already displayed signs of demographic onus during 2016–2020. Table 4 combined with predicted population and economic growth values for 2021–2025 in Taiwan,[6] computes that the growth rate of GDP per capita during this period consistently remains lower than the growth rate of GDP per worker, given the negative contribution rate. This not only aligns with the foundational definition, but also underscores the more sensitive and realistic interconnected effects between demography and economy. As time progresses, upon reaching the static age structure that formally signifies the demographic onus, the disparities between variables will further expand.

Table 4.
Economic performances synthesised different demographic bonus/onus definitions

	Labour Force Participation Rate (%)	Dependency Ratio (%)	GDP	GDP Per Capita	GDP Per Worker	Growth Rate of GDP Per Capita (%)	Growth Rate of GDP Per Worker (%)	Contribution Rate of Demographic Bonus (%)
2011–2015	74.07	35.01	512,451	21,958	29,606	23.5	21.2	1.5
2016–2020	72.46	38.02	604,835	25,664	35,410	16.9	19.6	−2.1
2021–2025*	69.54	43.80	684,971	29,158	41,922	13.6	18.3	−3.7

Note: 1. The gray highlighted cells signify the GDP contribution rate resulting from demographic transition. 2. *Denotes GDP forecast for 2021–2025 based on IMF "World Economic Outlook Database". Online: www.imf.org/en/Publications/WEO/weo-database/2021/October

Source: National Statistics, R.O.C. (Taiwan).

---

6   Population Projections for the R.O.C. (Taiwan). National Development Council. Online: https://pop-proj.ndc.gov.tw/dataSearch2.aspx?r=2&uid=2104&pid=59

5. Prospects and challenges of demographic development in Taiwan: The coexistence of population aging and sub-replacement fertility

Regarding future economic growth which is gradually slowing down in Taiwan, the impact of demographic onus is undoubtedly a serious challenge. Demographic onus arises from a diminishing proportion of the labour force and an elevated dependency ratio, encompassing two crucial endogenous driving forces: population aging and sub-replacement fertility.

5.1. Population aging

Many countries, particularly developed ones, face similar challenges of population aging to Taiwan. As the country experiencing the fastest population aging globally, Japan has witnessed a continuous and rapid increase in the size and proportion of its elderly population over more than half a century. The total population aged 65 and above has surged from around 5.4 million in 1960 to over 37 million in 2020, marking an increase of 6.9 times over 60 years. In terms of demographic structure, Japan has long surpassed the benchmark of a super-aged society. In 2020, the population aged 65 and above constituted approximately 30% (29.58%) of the total population.[7] Population aging inevitably accompanies the increased utilisation of medical resources, impacting Japan's social security system, particularly healthcare, long-term care and pensions, along with the local economies (Suzuki, 2023). In Taiwan, the average life expectancy at birth increased from 55.3 years in 1950 to 81.3 years in 2020, indicating the impending transition into a super-aged society (the proportion of the elderly population surpasses 20%). The total population of individuals aged 65 and above has steadily risen from around 0.16 million in 1950 to 1.92 million in 2000, and further to 3.79 million in 2020. Projections suggest it will reach 4.7 million by the year 2025. Moreover, there is a notable gender disparity in mortality rates during the elderly stage, with females increasingly dominating the population. The rapid feminisation of the elderly demographic suggests that the number of elderly widows will significantly increase in the future. The median age of the population in Taiwan has sharply risen due to the aging trend, going from 17.7 years in 1960 to 42.8 years in 2020, indicating that more than half of the population has entered middle age.[8]

A shortage of labour supply is a direct consequence of population aging on economic development. Population aging accelerates the aging of the labour force, resulting not only in a current reduction in the labour force, but also indicating a continuous decline in future supply. This reduction in the labour force affects productivity, subsequently

---

[7]   Population ages 65 and above (% of total population) – Japan. World Bank. Online: https://data.worldbank.org/indicator/SP.POP.65UP.TO.ZS?locations=JP

[8]   Population Projections for the R.O.C. (Taiwan). National Development Council. Online: https://pop-proj.ndc.gov.tw/dataSearch2.aspx?r=2&uid=2104&pid=59

impacting economic growth. According to the definition, the demographic bonus effect, driven by the growth of GDP per worker leading to the growth of GDP per capita, will gradually shift towards a reverse model of demographic onus.

The most serious impact of population aging is the increased financial burden on the public sector, along with a crowding-out effect on other policy budgets. Regarding medical insurance, population aging leads to a higher utilisation of medical resources in the island. Between 2000 and 2018, the proportion of medical utilisation by the population aged 65 and above rose from 28.8% to 38.2%, with expenditures growing by over 30%. In 2020, National Health Insurance expenditures exceeded 750 billion New Taiwan Dollars (1 NTD is approximately equal to 0.03 USD), with the elderly population's expenditures being 3.5 times that of the average population, imposing immense pressure on the healthcare system.[9] Between 1951 and 1971, the elderly dependency ratio in Taiwan hovered around 5%, meaning that every 20 working-age individual supported an elderly person (Department of Population Affairs, Ministry of the Interior [Taiwan], 2013). However, by 2020, the dependency ratio had surged to 23%, implying that every 4.3 working-age individual were required to support a single elderly person. According to government estimates, by 2025, as Taiwan enters a super-aged society with the population born during the baby boom retiring, the elderly dependency ratio will approach 30%, requiring the support of every 3.3 individual for one elderly person.

Meanwhile, the number of individuals with dementia and disabilities within the elderly population are increasing. In 2020, there were approximately 760,000 individuals with disabilities requiring long-term care. It is estimated that by the year 2026, this number will escalate to one million, reflecting a 30% increase (Department of Population Affairs, Ministry of the Interior [Taiwan], 2013). On the other hand, influenced by the traditional mindset, family units primarily serve as caregivers for disabled individuals. In terms of provision, taking care of one disabled member requires up to 9.9 years, incurring average costs of up to 4.85 million NTD (Chen, 2016). The long-term care of the elderly population has become a heavy burden on both working-age population and families. The proportion of females leaving jobs due to caregiving responsibilities has significantly increased. For married couples in their prime working years, the conflict between career competition and caregiving responsibilities has further led to a displacement effect on fertility, resulting in an irreversible transition.

5.2. Sub-replacement fertility

The concept of sub-replacement fertility was initially introduced by the Japanese Government in the White Paper on the National Lifestyle in 1992 (Cabinet Office, 2004). It refers to the trend in which the number of newborns continues to decrease amid an overall decline in the fertility rate among childbearing-aged women. Sub-replacement fertility has significant impacts on various aspects of society and economic development, constituting challenges faced by developed countries worldwide.

---

[9] National Statistics, R.O.C. (Taiwan). Online: https://eng.stat.gov.tw/point.asp?index=1

The declining trend unveiled by sub-replacement fertility lacks standardised indicators. For instance, the post-war baby boom in Japan was extremely short, lasting only from 1947 to 1949. After this brief period, the fertility rate started to decline sharply. Over the decade from 1947 to 1957, the total fertility rate dropped by over 50%, with the average number of children born per woman decreasing from 4.54 to 2.04 (Ogawa et al., 2005). By 1975, the fertility rate had fallen below 2.0, and in 1989, Japan hit its historically lowest rate at a "shocking 1.57". Demographic decline became a prominent public issue in Japanese society. By 2003, the total fertility rate had dropped to 1.29, earning Japan the label of a "ultra-low fertility" country (Tsuya, 2017). In Taiwan, the process of entering sub-replacement fertility involved surpassing several statistical benchmarks. In 1983, the total fertility rate first dropped below the replacement level. The total fertility rate was 1.23 in 2003, lower than that of Japan, earning it a place among the United Nations' ranks of the ten polities with the lowest fertility rates. Starting from 2019, Taiwan's total fertility rate has become the lowest in the world.

Sub-replacement fertility and population aging mutually reinforce each other in a negative spiral during demographic transition, displaying a seesaw effect where one end descends while the other ascends. This phenomenon is illustrated by the curve of the overall dependency ratio of the young and the elderly (Figure 5). The burden first decreases and then increases over time. In Taiwan, the pivotal moment in the dependency ratio occurred in 2014. Projections indicate that by 2050, every 1.5 working-age individual will support one elderly person, marking a threefold increase compared to the present. This burden is reflected in the financing of social security systems. Calculations based on the concealed liabilities of the social security systems reveal a staggering 18 trillion NTD currently. This indicates that by 2020, each of the 2.96 million ndividual under 14 years old in Taiwan would carry a liability of over 6 million NTD in these funds, highlighting the severe reality of the intensified pressure on the young generation due to the combined effects of sub-replacement fertility and population aging (Wang, 2017).

Frank Schirrmacher argued that sub-replacement fertility has far-reaching implications for human society. Families, which serve as the foundation of social cohesion, would be the first to endure the impact of the transition. In a context where family sizes are shrinking, the absence of future generations would impede the transmission of life values such as accomplishments and happiness. With the perpetuation of family eroding, younger generations either opt not to have children or have only one child, thereby fostering intergenerational effects. Consequently, existing social networks and orders are exposed to the risk of collapse (Schirrmacher, 2008). Chang and Song (2010) describe "compressed modernity" as the occurrence of contemporary economic, political and cultural changes in an extremely condensed manner across both time and space. The dynamic coexistence of mutually disparate historical and social development elements leads to the creation and reconfiguration of a highly complex and fluid social system. The practice of compressed modernity is evidenced in the evolving values of family and marriage in Taiwan.

5.3. Demographic transition and value change

The main factors influencing the decline in fertility rates in Taiwan from 1950 to 2020 have varied over time. In the 1950s, the decrease in the total fertility rate stemmed from a decline in the marriage fertility rate, especially a significant reduction in the probability of giving birth to three or more children. From the 1980s, the increasing age at first marriage became the primary factor for the decline in fertility rates. Higher education and increased female employment escalated the opportunity costs of childbearing. After 2000, the elevated average age for giving birth to the first child emerged as the dominant factor. The combination of stagnant wages and a prevailing pessimistic economic outlook among the childbearing-aged population greatly impacted decisions regarding fertility. In 2020, the average age of first marriage for women in Taiwan was 30.3 years, while the age for giving birth to the first child was 31.1 years, significantly higher than in most Asian countries (Gender Equality Committee, 2020).

The values associated with marriage and childbearing, which inherently drive changes in the fertility rate, have undergone significant transformations over the past 70 years. In studies addressing the ultra-low fertility rates in East Asia, Gavin Jones pointed out a deeper underlying concern behind low fertility rates, namely the atmosphere of "flight from marriage". Young people choose to evade marriage due to the challenging surroundings of establishing households (Jones, 2005). He argues that East Asian cultures still retain marriage and childbearing values of "selecting marriage", exemplified by the prevalent concept of "hypergamy", where individuals and their families seek upward social mobility through marriage. In this context, involuntary singleness will become more widespread in the era of sub-replacement fertility, leading to serious consequences of childlessness. Furthermore, macro-socioeconomic determinants such as job insecurity, work-family conflicts, the desire for high-quality offspring, and the insufficiency of government policy support have collectively reduced the willingness of married couples to raise children (Jones, 2008). On the other hand, the report from Taiwan's Ministry of Health and Welfare on Elderly Conditions indicates that approximately two-thirds of the population aged 65 and above reside in two-generation, three-generation, or even four-generation households. Compared to other aging countries, Taiwan demonstrates a relatively distinctive strength in family support, suggesting that social norms concerning family caregiving responsibilities and the traditional cultural emphasis on filial piety still exert influences over the care provided to the elderly population (Ministry of Health and Welfare, 2017).

6. Conclusion

Between 1950 and 1970, Taiwan relied on resources for agricultural and industrial development from the United States, providing an annual average of $100 million in assistance known as the US Aid. The reduction of dependency on new births emerged as an effective medium for capital accumulation and growth, aiming to accelerate Taiwan's self-sufficiency, alleviate the burden of US Aid, and transform Taiwan into

a labour hub for the US capital in East Asia. In 1959, Jiang Menglin, Director-General of the Sino-American Joint Commission on Rural Reconstruction (JCRR), wrote the famous essay, *Let's Confront the Urgent Issue of Taiwan's Population,* marking the inception of family planning and birth control policies on the island. The sustained decline in Taiwan's total fertility rate obviously contributed to the subsequent economic take-off (Tsai, 2007). The demographic bonus that began after 1990 was the final stage where demographic factors positively impacted economic growth. As shown in this article, the bonus stage ceased to exist by the 2020s. Conversely, the decline in fertility rates is a major cause of rapid population aging. In the early 1990s, Taiwan shifted from the traditional focus on birth control in family planning to the New Family Plan, prioritising the enhancement of population quality. Simultaneously, efforts were made to implement welfare policies to alleviate the challenges of marriage and raising children. These policies include instruments such as flexible working hours, paid leave, and childcare services that aim to improve the quality of family life. However, countering the forces leading to low fertility rates need to be assessed within the broader context of family policies, requiring the adjustments of entrenched cultural, institutional and familial arrangements, all of which are challenging to achieve (Jones & Hamid, 2015). Despite these endeavours, fertility rates have continued to decline, and population aging has become an irreversible structural transformation.

In addition to interventions targeting actual fertility behaviour, Taiwan is also committed to devising policies to increase the labour force and to minimise its contraction. Policy tools include extending working life, raising female labour force participation rate (LFPR) and enabling more workers to move from part-time employment into full-time employment, to address the adverse consequences of demographic onus (Jones, 2019). Besides, the rigid standard defining the age of elderly population has led to increasing adaptation challenges in the labour market and the functioning of social security systems. To address these problems, several aging countries have redefined the age criterion for classifying the elderly population. For example, Japan passed the Law Concerning Stable Employment of Older Persons in 2021, officially extending the legal retirement age for employees to 70. In the case of Taiwan, if the age definition of the elderly population is raised from the current 65 to 70, the adjusted proportion of the elderly population will remain below 20% over the next 15 years. This change could potentially sustain the demographic bonus phase until 2041.[10] Certainly, the issue of redefining the age of the elderly population is a considerable societal engineering that necessitates political leadership, professional expertise, widespread consensus and collaboration across economic sectors. Balancing the overall governance sustainability of the economic-social system will be a major goal and challenge for Taiwan's demographic policy in the future.

In rapidly aging economies, the gradual shortage and changing age structure of the labour force will drive the need for enhancements in individual productivity and auto-mation. Given the global industrial trend towards innovative technologies such as artificial intelligence and Taiwan's reliance on the ICT industry, further developing

---

[10]   Population Projections for the R.O.C. (Taiwan). National Development Council. Online: https://pop-proj.ndc.gov.tw/dataSearch2.aspx?r=2&uid=2104&pid=59

the demographic bonus – the demographic quality divide – is crucial for Taiwan's future demographic transition and economic development. The primary feature of the demographic quality dividend is the steadily increasing ratio of labour capital investment to the working-age population (Mason et al., 2016). This evolution shifts the focus of the labour factor from mere quantitative changes to significant qualitative leaps, promoting a technology and innovation-driven "intensive" perspective on demographic transition (Wang, 2021). Enhancements in the quality and productivity of the labour force can, to some extent, mitigate the impact of its relative numerical decline. Based on Figure 6, the increase in savings among the working-age population has promoted substantial investments in human capital, primarily through educational expenditure. Such capital deepening is the core driving force behind the formation of the demographic quality dividend. By raising the knowledge and skill levels of the educated population, the quality of the labour force can be enhanced, thus flourishing the labour force mobility (Zhou et al., 2023). This is conducive to the market-oriented allocation of labour resources and alleviates the lurch of "technological unemployment" (Jafrin & Masud, 2020) caused by the application of updated technologies in the workplace, leading to an improvement in the labour employment rate, including the elderly labour population. In recent years, the Taiwanese government has enacted the core strategic industries plan and policies strengthening the cultivation of digital talents, thereby optimising the demographic quality dividend. This article reveals that the early policies that "served" economic development have generated new demographic outcomes due to economic growth, triggering a new phase of adjustment and planning. The interplay between demographic transition and economic development has evolved into an ongoing feedback loop, constituting a mutually reinforcing cycle of policy dynamics, which is also a rich field for future researchers to delve in further empirical studies of Taiwan.

References

Baba, S. (1993). The Super Aged Society. *World Health, 46*(3), 9–11.

Barclay, G. W. (1954). *A Report on Taiwan's Population to the Joint Commission on Rural Reconstruction*. Princeton: Office of Population Research, Princeton University.

Bloom, D. E. & Williamson J. G. (1998). Demographic transitions and economic miracles in emerging Asia. *The World Bank Economic Review, 12*(3), 419–455. Online: https://doi.org/10.1093/wber/12.3.419

Bloom, D. E., Canning, D. & Sevilla, J. (2003). *The Demographic Dividend. A New Perspective on the Economic Consequences of Population Change.* RAND Publications.

Cabinet Office, Government of Japan (2004). Measures for an Aging Society with a Decreasing Fertility Rate (これまでの少子化社会対策の経緯). Online: https://tinyurl.com/ydmjrydn

Chang, K. S. & Song, M. Y. (2010). The stranded individualizer under compressed modernity: South Korean women in individualization without individualism. *British Journal of Sociology, 61*(3), 539–564. Online: https://doi.org/10.1111/j.1468-4446.2010.01325.x

Chang, M. C. & Lee, M. H. (2001). Fertility Trends in Below-Replacement Levels. *Journal of Population Studies, 23,* 93–112.

Chen, C. N. & Liu, K. C. (2007). Is Taiwan's Lowest-low Fertility Reversible via Socio-economic Development? *Journal of Population Studies, 34,* 1–36. Online: www.psc.ntu.edu.tw/jps/pub/34/assets/1.pdf

Chen, J. P. (2016). *Demographic Dividend, Aging Society and Inclusive Growth*. Beijing: Economic Science Press.

Chen, Y. H. (2008). Demographic Dividend and China's Economic Growth. *Journal of Jiangsu Administration Institute, 4,* 58–63.

Chen, Y. & Ye, W. Z. (2013). Dynamic Relationship between Aging and Evolution of Industrial Structure in Taiwan. *Population Journal, 35,* 63–72.

Chen, Y. M. (2016). A Triple Win Strategy for Long-Term Care: Family Caregiver Support Services. *Community Development Journal, 153,* 199–213. Online: https://cdj.sfaa.gov.tw/Journal/FileLoad?no=179916

Chiang, M. H. (2023). Taiwan Semiconductor Manufacturing Company: A Key Chip in the Global Political Economy. *East Asian Policy, 15*(1), 36–46. Online: https://doi.org/10.1142/S179393052300003X

Deaton, A. & Paxon, C. (1999). *Growth, Demographic Structure, and National Saving in Taiwan*. Working Paper No. 224. Research Program in Development Studies, Princeton University. Online: https://shorturl.at/8Yr3W

Department of Population Affairs, Ministry of the Interior (Taiwan) (2013). *Population Policy White Paper. Fewer Children, Population Aging and Immigration*. Online: www.ris.gov.tw/documents/data/en/4/Population-Policy-White-Paper.pdf

Freedman, R. (1986). Policy Options after the Demographic Transition: The Case of Taiwan. *Population and Development Review, 12*(1), 77–100. Online: https://doi.org/10.2307/1973352

Gender Equality Committee, Executive Yuan (Taiwan) (2020). *Annual date of average age of first marriage and first childbirth for women*. Online: https://shorturl.at/scmfc

Hale, E. (2021, November 2). Taiwan's tech boom masks a daily struggle for the masses. *Nikkei Asia*. Online: https://shorturl.at/iMipM

Huang, D. X., Liu, B. J. & Young, Z. H. (2014). *The Stagnation of Real Wages in Taiwan: Global Trends and Taiwanese Characteristics*. IEAS Working Paper. Academia Sinica: Taiwan. Online: www.econ.sinica.edu.tw/~econ/pdfPaper/14-A012.pdf

Huang, W. H., Lin, Y. J. & Lee, H. F. (2019). Impact of Population and Workforce Aging on Economic Growth: Case Study of Taiwan. *Sustainability, 11*(22), 6301. Online: https://doi.org/10.3390/su11226301

International Labour Organization (2013). *Wages and equitable growth. Global Wage Report 2012/13*. Geneva: International Labour Office.

Jafrin, N. & Masud, M. M. (2020). The Demographic Dividend and Economic Growth: An Integrated Theoretical Framework. *Demografie, 62*(4), 240–252. Online: https://shorturl.at/mfybL

Jin, X. T. & Dai, M. H. (2012). Analysis on the Impact of Population Aging on Economic Society in Taiwan Area. *Population Journal, 5,* 72–80.

Jones, G. W. (2005). The "Flight from Marriage" in South-East and East Asia. *Journal of Comparative Family Studies, 36*(1), 93–119. Online: https://doi.org/10.3138/jcfs.36.1.93

Jones, G. W. (2007). Delayed Marriage and Very Low Fertility in Pacific Asia. *Population and Development Review, 33*(3), 453–478. Online: https://doi.org/10.1111/j.1728-4457.2007.00180.x

Jones, G. W. & Hamid, W. (2015). Singapore's pro-natalist policies: To what extent have they worked? In R. R. Rindfuss & M. K. Choe (Eds.), *Low and lower fertility: Variations across developed countries* (pp. 33–61). Springer.

Jones, G. W. (2019). Ultra-low fertility in East Asia: policy responses and challenges. *Asian Population Studies, 15*(2), 131–149. Online: https://doi.org/10.1080/17441730.2019.1594656

Li, S. M., Chen, K. J. & Tu, J. C. (1990). Population Growth and Economic Development: A Critical Review. *Journal of Population Studies, 13,* 107–124. Online: www.psc.ntu.edu.tw/jps/pub/13/assets/6.pdf

Lin, C. H., Wang, K. C. & Hsu, C. P. (2010). Population Aging, Forecast of Labor Supply, and Effect on Asset Demand: The Empirical Analyses of Taiwan. *Chang Gung Journal of Humanities and Social Sciences, 3,* 171–219. Online: http://cgjhsc.cgu.edu.tw/data_files/3-1%2007.pdf

Lin, H. C., Lee, H. L., Hsu, S. M., Lin, K. J., Lee, D. H., Chang, C. C. & Hsu, S. H. (2015). Baseline Forecasting for Taiwan's Population in the Face of Low Fertility Rate and Ageing Problems. *Taiwan Economic Forecast and Policy, 46,* 113–156. Online: https://ir.sinica.edu.tw/handle/201000000A/58007

Lin, Tung-Fa. (2018). Population Migration of Taiwan in the Early Post-War Period to the 1950s. *Newsletter of Taiwan Studies, 103,* 4–7. Online: https://wwwacc.ntl.edu.tw/public/Attachment/811615572091.pdf

Mason, A., Lee, R. & Jiang, J. X. (2016). Demographic Dividends, Human Capital, and Saving. *The Journal of the Economics of Ageing, 7,* 106–122. Online: https://doi.org/10.1016/j.jeoa.2016.02.004

Ministry of Health and Welfare (Taiwan) (2017). *Report of the Senior Citizen Condition Survey.* Online: https://shorturl.at/2RQ0t

Misra, R. (2015). Impact of Demographic Dividend on Economic Growth: A Study of BRICS and the EU. *International Studies, 52*(1–4), 99–117. Online: https://doi.org/10.1177/0020881717714685

Mueller, E. (1972). Economic Motives for Family Limitation: A Study Conducted in Taiwan. *Population Studies, 26*(3), 383–403. Online: https://doi.org/10.1080/00324728.1972.10405909

Mueller, E. (1977). The Impact of Demographic Factors on Economic Development in Taiwan. *Population and Development Review, 3*(1–2), 1–22. Online: https://doi.org/10.2307/1971757

Ogawa, N., Kondo, M. & Matsukura, R. (2005). Japan's Transition from the Demographic Bonus to the Demographic Onus. *Asian Population Studies, 1*(2), 207–226. Online: https://doi.org/10.1080/17441730500317451

Peng, S. L., Kuo, N. F., Chou, J. & Fang, W. H. (2009). The Impact and Evaluation for the Age Structure, Income Distribution and Industrial Structure on Taiwan's Consumption and Output. *Taiwan Economic Forecast and Policy, 39,* 51–101.

Sanchez-Romero, M. (2009). *Demographic Transition and Rapid Economic Growth*: The Case of Taiwan. Working Paper. Center on the Economics and Economics of Aging (CEDA), University of California: Berkeley. Online: https://paa2009.populationassociation.org/papers/90928

Schirrmacher, F. (2008). *Minimum. Vom Vergehen und Neuentstehen unserer Gemeinschaft.* Karl Blessing Verlag.

Suzuki, Y. (2023). Impact of Japan's Aging Population in 2030: Focusing on the Effect on the Social Security System and Local Economies. *Mitsui & Co. Global Strategic Studies Institute Monthly Report,* 1–8. Online: https://tinyurl.com/2bhnc6ee

Tsai, H. J. (2004). The Analysis of Regional Political Economy on Taiwanese Immigration. *Review of Global Politics, 7,* 111–130. Online: https://doi.org/10.29899/JRM.200407.0006

Tsai, H. J. (2007). Historical Formation of Population Policy in Taiwan. *Taiwanese Journal of Sociology, 39,* 65–106. Online: https://dx.doi.org/10.6786/TJS.200712_(39).0002

Tsai, I. J., Chu, C. Y. & Chung, C. F. (2000). Demographic Transition and Household Savings in Taiwan. *Population and Development Review, 26,* 174–193. Online: www.jstor.org/stable/3115216

Tsuya, N. O. (2017). Low Fertility in Japan—No End in Sight. *Asian Pacific Issues, (131),* 1–4. Online: www.eastwestcenter.org/sites/default/files/private/api131.pdf

Tung, S. L. (1984). An Econometric Analysis of The Effects of Population Change on Economic Growth: A Study of Taiwan. *Applied Economics, 16*(4), 523–538. Online: https://doi.org/10.1080/00036848400000067

United Nations Population Fund (UNFPA) Viet Nam (2010). *Taking Advantage of the Demographic Bonus in Viet Nam. Opportunities, Challenges, and Policy Options.* Online: https://vietnam.unfpa.org/sites/default/files/pub-pdf/Demographic_Bonus_Eng.pdf

Wang, F. & Mason, A. (2006). Demographic Factor in China's Transition. *Chinese Journal of Population Science, 3,* 2–18. Online: https://doi.org/10.1017/CBO9780511754234.006

Wang, J. M. (2017). On the Aging Population and the Declining Birth Rate in Taiwan and Their Implications for Economic and Social Development. *Journal of Beijing Union University, 15,* 52–58. Online: https://doi.org/10.16255/j.cnki.11-5117c.2017.0042

Wang, S. (2021). The Second Demographic Dividend and Economic Growth: Theories, Mechanisms, and Simulations. *Population Research, 45,* 82–97.

Yu, Z. X. & Wang, J. L. (2009). *Population Changes and Economic Development in Taiwan.* Taipei: Linking Publishing Company.

Zhou, J., Deng, J. J., Li, L. & Wang, S. (2023). The Demographic Dividend or the Education Dividend? Evidence from China's Economic Growth. *Sustainability, 15*(9), 7309. Online: https://doi.org/10.3390/su15097309

This page intentionally left blank.

The Perspectives of Family Foster Care in the Czech Republic, Hungary, Poland and Slovakia

Mária Herczog*⊙

---

* Chair, Family, Child, Youth Association, Budapest, Hungary; President, Missing Children, Brussels, Belgium, e-mail: herczogmaria@me.com

Abstract: Reforms of the child protection systems, provision of family- and community-based alternative care has been developed to a certain level in all countries in Central and Eastern Europe and has increased the role of care provided by foster families replacing institutions to ensure that the best interests principle is taken into consideration when children are separated from their families. The research describes the foster care system in the so-called Visegrád countries: the Czech Republic, Hungary, Poland and Slovakia, and the results based on at least 50 interviews in each country conducted by local experts on subjective well-being of foster parents, their perceptions about their roles and place in their respective countries and their needs. The article includes the legal framework, recruitment, preparation and support to foster families, their subjective well-being and needs in the four countries, including the history of their child protection systems to better understand the current situation. The outcomes show differences in approach to foster care, the perception on the roles, responsibilities and needs based on the different traditions, earlier and current policies and practices. Understanding the attitude changes related to the rights of children, those in vulnerable situations, and to their families of origin would be essential to further develop and improve the child welfare and protection systems, and listening to children on their perceptions and the realisation of their rights.

Keywords: child protection, foster care, foster parents, children's rights, V4 countries

1. Introduction and background

The UN General Assembly Resolution on the Promotion and Protection of the Rights of Children in December 2019, in line with several earlier UN treaties, guidelines and recommendations, recognises that children should grow up in a family environment to have a full and harmonious development of their personality and potential; urges member states to take actions to progressively replace institutionalisation with quality

alternative care and redirect resources to family and community-based services; and calls for "every effort, where the immediate family is unable to care for a child with disabilities, to provide quality alternative care within the wider family, and, failing that, within the community in a family setting, bearing in mind the best interests of the child and taking into account the child's views and preferences" (UN General Assembly, 2020, cited by Goldman et al., 2020, pp. 606–607). The recommendations based on the general day of discussion on children's rights and alternative care organised by the UN Committee on the Rights of the Child (2021) reiterate the importance ensuring that all children grow up in safe and nurturing families, and all families should have the support they need to provide safe, nurturing and loving environment for children. It requires comprehensive policies and programmes, prioritisation of universal, non-discriminatory social services, focusing on early identification, enhancement of parenting skills, intervention for families at risk of separation, timely access to services for families promoting inclusion and participation in the community.

These recommendations suggest prioritising the needed support to families of children, to prevent unnecessary separation, to protect children who are deprived of parental care by providing high-quality family-based alternatives within the community, to recognise the harm of institutionalisation, and to strengthen systems for the care and protection of all children in line with the UN Convention on the Rights of the Child (UNCRC, 1989). Concerted global efforts to reform systems for the care of children by keeping families together by strengthening families and building up family support services in communities, putting in place alternative family-based care, and progressively replacing institutional care with quality alternatives in a safe and structured manner are under way and should be promoted (UN General Assembly, 2020).

The study presented describes the foster care system in the four countries and the results based on the interviews conducted on subjective well-being of foster parents, their perceptions about their own roles and place in their respected countries and service provider and their needs in the so-called Visegrád countries, in the Czech Republic, Hungary, Poland and Slovakia.

Several studies have been revealing the commonalities and diversities in foster care in the last decades in Europe, but they have not covered many areas, nor all the countries effected. Overviews of the developments in Europe, with special focus on the transition countries were published among others by Tobis (2000), Vecchiato et al. (2002), Browne et al. (2005), UNICEF (2013), Anghel et al. (2013), Eurochild (2019). The needs of foster parents including training, motivation, attitude and satisfaction in different countries have also been explored from different perspectives and in different countries, regions, among others, by Whenan et al. (2009), Kaasbøll et al. (2019), Neagoe et al. (2019).

Despite of the efforts made, still hundreds of thousands of children are living in institutions, although the number of children in kinship and foster care is growing across Europe (Eurochild, 2019). Many countries in the region have increased their efforts to promote family-based care for children and have sharply reduced their reliance on institutions (UNICEF & Eurochild, 2021). The European Expert Group on the Transition from Institutional to Community-Based Care has produced material to

support the reforms (European Expert Group, 2012; 2014), and the funds made available for the countries to implement the needed reforms and changes have also generated substantial activity.

The reforms of the child welfare and protection system, known as de-institutionalisation, have been focusing in many countries on the implementation of the best interests principle among other efforts, increasing the role of family support, local, community-based services, prevention, gatekeeping and reintegration of children into their families of origin if possible and closing the institutions, 'children's homes'. Based on the experience of western countries and many foreign NGOs and experts helping to develop new child welfare and protection policies, foster care has become one of the main channels to place children into families and avoid institutional placements in many countries following the political-economic changes in 1989.

2. Historical background and the development of the child protection systems in the Visegrád countries

There are many similarities, but also important differences based on the history, traditions, culture and diverse impacts explaining why the child welfare and protection systems have evolved differently in the different countries in all regions, including in those covered by this project. All four countries have become members of the European Union in 2004, with social policy, health and education remaining the competencies of the individual countries, while there are several instruments to support the required changes in policies and practices. The countries investigated in this study belonged to the former Soviet bloc countries, following the patterns of the Soviet, state-run model of child protection, prioritising institutions to family-based foster care, believing that professionals can take better and more transparent care of children in state-run services than lay families, believed to be more conservative and not representing the new ideas of child rearing. Following the transition in 1989, changes in their respective approaches and systems have been very different, just as in other areas of social policy.

2.1. The Czech Republic

In the first decade of the 20th century, a separate educational system and local child protection services supported families with children under 3, and were provided in the same way as medical counselling and daycare. Efforts were underway already at this time to integrate different services into a common system; however, these were not completed. The current child protection system can be traced back to these early developments, together with the establishment of institutionalisation and segregation. While kinship and foster care were the dominant forms of care for children in this early period, children with disability and Roma children had been excluded and placed in institutions already from 1921, based on the new legislation, which remained unchanged until the forties. During the German occupation (1939–1945) institutionalisation was preferred

just like in Nazi Germany, with the number of children in institutions increasing substantially partly due to the death of the parents and abandonment, and residential homes being supervised by German authorities and some NGOs.

After WWII, a medicalised concept became dominant, especially in the cases of children with disabilities, and supervision of the residential homes belonged to the Ministry of Health. Until the political-economic changes in 1989, the Soviet institutional approach was exclusively used, to ensure "the public interest to prevent such situations as breaches of upbringing and lack of parental control of children which leads to the incomplete internalization of socialist morality" (cited by Schmidt & Bailey, 2014, p. 59). Family-based alternatives were not used in any form (Truhlárová & Levická, 2012).

Alternative care today still includes different types of institutions (infants' homes, diagnostic institutes, children's homes, residential schools and secure children's homes), various family-type placements, including four forms of foster care. Official estimates indicate that approximately 23,000 children are accommodated in over 200 residential homes for children, including a high number of young children under the age of 3, waiting for a court decision, which can last several months. Between 1990 to 2010, the number of children placed in residential facilities has increased from 704 to 1,268 per 100,000 of the child population (UNICEF, 2012).

Despite the numerous legislative changes, recommendations and international efforts, the number of children in alternative care has increased in the last twenty years, with preference being given to institutional placements, while early support and prevention centres and local services have also been established.

The new legislation in 1999 on the social and legal protection of children aimed at identifying families at risk, collecting information among various actors, providing support to parents and options for the right to be heard, and initiating legal action if needed. Local authorities under the special department in the Ministry of Labour and Social Affairs were designated to implement the law. Instead of focusing on prevention and early support, the new activities consisted in crisis intervention and after-crisis placement of children as the main activity, and dealing with families in vulnerable situations.

As a result of the external pressure to start the de-institutionalisation of children, the National Action Plan for Transformation and Unification of the System of Care for Children at Risk was introduced in 2009, yet without implementation. The large institutions have been re-modelled and smaller units established but the dominant form of care remained.

Despite the National Strategy to Protect Children's Rights and the National Action Plan for 2012–2015, de-institutionalisation has not shown much progress. The reasons identified include the lack of political commitment and acceptance of the need of children, lack of adequate community-based services despite the growing need, and a lack of cooperation between different ministry departments and communities providing services. Insufficient prevention and gatekeeping efforts and a very strong lobby of professionals, primarily paediatricians favouring residential placements instead of family-based care prevents the changes. The number of applications for foster care has decreased due to the higher demands as far as preparation and contact with the biological families is concerned (Lumos, 2018).

The debate on closing all infant homes and replacing them with temporary foster families, besides supporting families at risk and preventing the out-of-home placements has been going on in the Czech Republic for almost 20 years. It is one of the last European countries where it is still possible to place a child younger than three years in an institution. Infant homes are health service facilities, under the jurisdiction of the Ministry of Health, and provide paediatric services. A new Strategy for the Protection of Children's Rights 2021 to 2029 was adopted by the Czech Government in December 2020, followed by an Action Plan for its implementation during the first half of its term, therefore in force from 2021 to 2024. The strategy and action plan determined a strategic framework and a basis for closing the infant homes until the end of 2024. Further achievements are seen in the ongoing legal procedure connected to the amendment of the Act on the Social and Legal Protection of Children. The National Strategy was created in cooperation with a wide representation of professionals, children's groups, families and a wide range of civil society organisations, including an umbrella institution representing over 80 non-governmental organisations (OHCHR, 2021). An amendment to the Act on Health Services prohibited the placement of children under the age of 3 in institutional care, with the exception of children with severe disabilities and sibling groups (Fundamental Rights Agency, 2023).

The majority of funding during the last years was still spent on institutions (52%), less than a third to foster care, and only 19% on prevention and working with families in 2017. The main stakeholders, ministries responsible for the different areas of child welfare and protection have not agreed on the required solutions (The League of Human Rights, 2017). At the end of 2022, 12,268 children were placed in foster families permanently and 535 temporarily, 403 children placed in temporary homes for urgent needs, 818 under the age of three in infant homes, 4,994 children in residential homes, of whom 350 were over 18 years of age, 980 children in homes for children with serious behavioural problems (Ministry of Labour and Social Affairs, cited in Fundamental Rights Agency, 2023).

2.2. Hungary

The first child protection legislation adopted by Parliament in 1901 was a very comprehensive law, acknowledging the responsibility of the State for the care of children in need. Almost all children under 15, apart from the severely disabled and children in conflict with the law were placed in foster care (95%), and this remained the case until the end of WWII. The post-war era emphasised more professional, controlled provisions leading to a gradual decrease in foster care, based on the belief that institutional facilities better serve the developmental needs of children. Trained staff working in teams was considered more aligned with the new politics than the mostly uneducated families who were fostering without monitoring and seen to transfer undesirable values to children.

Besides large residential homes often placed in castles confiscated from the old bourgeoisie in the late 1940s, children's towns were established accommodating hundreds of children separated according to their age and gender, even siblings within the closed

compounds. Foster care placements accommodated less than 20% of all children in alternative care.

By the mid-1980s it became clear for many professionals and decision-makers that institutions could not provide the care and personal relationships children needed. In 1986, social work education was re-established, and a new program of social pedagogy was also introduced. The Ministry of Social Affairs and Labour initiated a national pilot program providing experimental training for foster parents with external experts. The aim was to employ professional foster parents, as relying on voluntary provision was not an option in an economic system based on two incomes per family, and the lack of voluntary work in general.

Three SOS Children's Villages were also opened in the late 1980s providing an in-between model with much higher standards, based on international support and management. The reform efforts were not welcome by all and the closure of the first three infant homes in 1988 in Pest County had generated strong resistance from the residential care lobby, particularly among the infant home representatives (Herczog, 1997).

The political and economic transitions after 1989 have further slowed the process of reform, as other major changes were given priority. The legislation on child protection and custodian management in 1997 followed the principles of the UNCRC ratified by Hungary in 1991, and the most up-to-date good practices. The establishment of local, community-based child welfare services aiming at preventing the need for out-of-home care and working in cooperation with other sectors and professionals, including NGOs, could have ensured proper early support and gatekeeping mechanisms in place. The closure of several large residential homes for children, recruiting and training foster families and establishing smaller group homes accommodating not more than 12 children seemed to modernise child welfare and protection. An initiative in 1996 was aiming at the experimental pre-service training for prospective Roma foster parents so that Roma children, highly overrepresented in the care system, could be placed with families ensuring their identity and culture. The successful program resulted in recruiting the first fourteen professional Roma foster families. Since then an estimated 5% of all foster parents are of Roma origin, which is still a unique opportunity in the CEE region (Diósi, 1993).

However, the inadequate resources allocated, lacking the time for a smooth transition, for the preparation of those working in the old regime and raising public awareness of the changes occurring, together with the different conflicts of interests at many levels have resulted in very mixed outcomes. After the first years of significant changes of the decreasing referrals of children and the development of local service provision, since 2008 the trend has somewhat changed. The number of children has not decreased further, despite the decreasing birth rate, the local services have not got sufficient resources, the share of church-run services has increased in all forms of care, though residential homes are still dominantly state-run by a centralised authority (SZGYF), and the quality of care in the child protection system has worsened. Foster parents are contracted and paid by the service providers, 19 of the 22 organisations offering foster care belong to church-run NGOs, accommodating 98.4% of the children (SzocOkos, 2023). Fostering has increasingly become an option for those in need of income, lacking employment opportunities, and due to the lack of applications, the conditions have been significantly

worsened by the placement of over 60% of the children in settlements with less than 2,000 inhabitants, lacking the basic services, often even GPs, health visitors, kindergartens and schools. The number of foster parents has remained roughly the same, 5,811 in 2023, accommodating 70% of the children. By the end of 2023, there were 15,922 children under the age of 18 in family foster care and 7,293 in residential care, while 2,387 young people older than 18 in after-care both in foster families and in residential facilities (Hungarian Central Statistical Office, 2024).

The new regulations introduced in 2014 allow for the placement of a child under the age of 12 in residential homes in exceptional circumstances only; however, still many children even under the age of 3 are in children's homes. The regulations are permitting larger sibling groups and severely disabled children to be placed in residential homes, regardless of their age. Reunification of children with their families is very rare due to the lack of capacities of local services and the absence of political commitment to support poor and deprived families. According to a recent investigation of the Commissioner for Fundamental Rights, at least 35% of children are placed in alternative care because of poverty and lack of support, despite the clear prohibition in the law to remove children from their families because of material deprivation only. Roma children are highly overrepresented in alternative care and placed in residential homes in large numbers, just like children with disabilities (The Budapest Beacon, 2018; Eurochild, 2018).

Despite the increase in allowances and remuneration to foster parents, considering the inflation rate these resources are still not sufficient to cover the costs and provide a satisfactory income for them. According to the reports, at least 2,000 more foster families would be needed to accommodate children in need and replace institutional care. A recent worrying indicator of the lack of placement options is the growing number of newborns left in maternity wards, spending several months in hospitals, waiting for vacancy in foster families or infant homes (Muhari, 2024). The government has decided to ease the provisions to adopt children left alone, instead of providing prevention of unwanted pregnancies, support to families in need and expecting women, and providing hospital-based social work and psychological support to women so they do not abandon their newborns (National Assembly, 2024).

2.3. Poland

Before WWII, substantial developments ensured the care of children deprived of their family and the progressive work of Janusz Korczak and Babicki, among others, was characterised by the child-rights based approach already from the early years of the 20th century. Children's homes introducing self-governance and focusing on the individual, developmental needs of children were exceptional examples of good practice.

In 1921, the right to social assistance was acknowledged by the Polish Constitution "children without necessary care from their parents have the right to receive care and help from the government" (Article 103) (see Stelmaszuk, 2002; Kolankiewicz, 2006; Knuiman et al., 2015).

Similarly to the other countries of the region, following the German occupation during WWII and after the war, from the early fifties the child welfare and protection system was nationalised and the institutionalisation of children has become the main form of placement, services provided to families and placing children in foster care was not a priority. Since the modernisation of the care system in the 1970s, family support and foster care has become more accepted as the best place for children to be raised outside of their families of origin. Large residential homes were not seen as adequate placement for children any more, especially as the staff working there were not well trained, and contact with the families or the efforts to reunite children with their families were inadequate. The first regulation of foster care was introduced in 1979 (Łuczyński, 2007).

The Polish Act on Social Policy in 2004 provided that children can only be placed in residential homes in case the family is not able or willing to take care of them and there is no foster family available meeting the child's individual needs. The Family Assistance and Alternative Care Act was introduced in 2011, replacing former regulations. The newly established group homes can accommodate less than 14 children. However, this was achieved frequently by dividing former large institutions or building group homes, usually next to each other in large complexes, with EU structural funds used to create these settings. This is against the recommendations and professional standards of the European recommendations and the prohibition to spend the funds on residential facilities (see European Expert Group, 2012; 2014). Children under the age of 10 can be placed in residential homes in exceptional circumstances only. In 2017 there were still 3,200 children younger than 10 living in institutions.

Poland is one of the 12 countries in the European Union identified to enhance de-institutionalisation reforms. Foster care has become an essential option for children in alternative care; however, its quality and support of children are not satisfactory. In 2021, there were 121,225 children in alternative care, including 15,000 children with disabilities, 70,753 (65%) of them in foster families. Of 100,000 children under the age of 18, 1,788 are living deprived of their biological families (UNICEF & Eurochild, 2021). This number shows a steady decrease compared to the previous decade. It is important to note that in Poland the term 'foster care' encompasses both foster family-based care (up to three children per family) and institution-based care or a residential home where up to eight children are cared for by professional staff.

The number of foster families has dropped slightly, by 0.7%, in comparison with the previous year, partly due to the lack of public awareness, inadequate professional support and low remuneration to foster families. In the countryside and far from the cities the professional supervision of foster families is of low quality, lacking the support of psychologists and other specialists. Foster care supervisors are overburdened. Reunification of children with their biological families is challenging, as in most cases children stay in foster care for several years and contact with one's biological family is very limited. Foster parents in many cases do not support or encourage the relationship between the children in their care and the family of origin. NGOs and professionals working in the field have called for an update of the National Strategy on Family Foster Care as well as legislative changes to improve the situation.

2.4. Slovakia

The history of the child protection system between 1918 and 1993 was almost the same as in the Czech Republic, as Slovakia was part of Czechoslovakia. After becoming an independent State and joining the European Union in 2004, Slovakia has made substantial efforts to implement children's rights in a number of areas. However, minorities in the country have been facing severe deprivation, especially Roma, living in over 600 communities across the country.

Act No. 305/2005 Coll. on social and legal protection of children and social care defined the provision of care for children who are removed from their biological families and placed in alternative care. From 1 January 2009, the Act determines that every child under the age of 6 years should be placed in professional family care within restructured institutions. This form is a mixture of residential home and foster care, as within the institutions smaller group homes have been set up, where family-like life is imitated by professional caretakers, a couple or a single person, as quasi-foster parents. It is similar to the SOS Children's Villages model (see Moravkova, 2018).

Despite the decreasing number of children placed in institutions, in 2022 there were still 4,492 children living in residential homes (Ruszkowska & Lovašová, 2023), with Roma children being highly overrepresented among them, just like among the more than 700 children with disabilities also placed in children's homes, making three-fourth of all children without parental care. 8,695 children were accommodated in family foster care, but very few Roma children are accepted by foster families or the communities where they are living (UNICEF & Eurochild, 2021).

3. Findings

3.1. The Czech Republic

Fifty-eight long-term, non-kinship foster carers participated in the research. Half of them are taking care of one child, 27.5% for two children and 24.1% for three or more. 25 children are siblings, placed together in the foster families. 5 families are fostering 4 or 5 children, 26 families are taking care of children with special needs.

22 parents have been fostering for more than 10 years, 18 for 4–6 years, 6 for 1–3 years. Many foster families live in small settlements, 20 of them in villages with less than 2,000 inhabitants, 20 with less than 20,000 and 18 in larger cities, over 100,000 inhabitants. Almost 75% of the respondents are fostering couples, the others are individuals. Over 60% are employed full-time somewhere else while fostering.

The motivation for half of the respondents was to help children in need, 29% because of infertility, while some wanted to have a larger family. Half of them have received negative comments on their decision but in most of the instances the family and the broader network was also reacting in a positive or passive way.

They would have needed more information during the preparation on the background of children's families and the developmental delays, as well as practicalities. They found

group work very helpful, just like the knowledge and competency of the trainers for all the participants. All but 3 parents attended the PRIDE program, almost all regularly attend meetings, lectures, or have frequent supervision. In addition to professional support, one third of them can rely on regular family help, their partner and more than 10 persons also get help from friends if needed. Two-third of the carers would require more support from psychologists, therapy for children and helping them better understand the needs of the children in their care to respond in an adequate way. Seventeen foster parents would need more financial support, eight of them more supervision and vocational training.

Less than half of the foster carers participating in the project (44%) feel that their role does not differ from their everyday experience of parenting, while others perceive it as a mission, to provide good care and preparation for adulthood for children in need, providing secure attachment, with some mentioning the cooperation with professionals to fulfil their tasks.

They are suggesting other foster parents to connect and form networks, learning as much as possible about the child before the placement, and the different issues that might emerge, like the consequences of abandonment, behavioural problems and delayed development.

The greatest satisfaction for two-third of the foster parents responding is to do something useful. Others are happy taking care of children who need care and watching the children bonding (12%), their own self growth (9.8%), development or filling the gap "at the table of their own family" (8.5%).

Fifty respondents reported to have sufficient support from the health care services, some do not need them at all, and in cases of schools they have similarly positive experiences. Six parents were facing difficulties because of the children's behaviour or their "bad genetics", but did not want to share this problem with others.

Over two-third of the foster parents feel that their family cohesion and love help feeling satisfied with their role, and the development of a close relationship with the child and meeting their individual needs. At the same time, one fifth of the parents are struggling with behavioural problems of the children, and more than a third of them experience difficulties communicating properly with the children in relation to the special needs and developmental delays, or former trauma. Some families are facing problems to keep contact with the biological families, and with the low prestige of foster care. Almost all the foster parents would like to improve their skills and knowledge, helping secure attachment and long-lasting relationships for the children, supporting the development of those with special needs and some to help children of Roma origin to get better integrated.

3.2. Hungary

Fifty foster parents were interviewed, selected through expert sampling, representing all types of settlements (periphery – district centre – county centre cities – capital). Foster parents were contacted partly through foster care networks, or through county child

protection agencies, who informed foster parents about the project, recruited them, and provided the venue necessary for the interviews.

In Hungary there is no differentiation among foster parents based on the type or length of care. Most children spend long years in foster families, before being adopted, returning home, changing placement, or leaving care as adults, often including years of after-care periods as well.

Most respondents were foster mothers, only 3 foster fathers participated in the research. 32 respondents identified themselves as traditional foster families, the other 18 as formerly employed professional foster parents. 30 foster parents are living in marriage, 4 with a partner and 16 women are singles. More than half of them have primary education and some vocational training, one fifth has secondary and one fifth tertiary education.

Foster parents identified a few motivational factors which played a role in their commitment. One fifth of them have met foster care in their early childhood, either because their parents also fostered children in their own family, or because they had to foster a child from their own family at a young age. A lot of respondents claimed that fostering replaced parenting of their own children leaving home as adults, others reported about a personal linkage to a child left without family, or to other foster parents, leaving an impression and motivated them to take on fostering. A small proportion of respondents cited existential reasons, the lack of local employment opportunities as one (but not the only) reason for becoming a foster parent.

The first personal experience with foster parenting was mostly influenced by personal acquaintances: two-fifth of the respondents claimed that they first heard about fostering opportunity from a friend or from other foster parents. For 15 respondents the media (primarily local newspapers) raised awareness about fostering, while 10 persons met foster parenting already in their childhood.

Although – according to the interviews – foster parents participated in highly valued pre-service trainings, among others, all in PRIDE (called FIKSZ in Hungary), depending on what time they have engaged in foster care (and which training was compulsory in the given period), they agreed that the information provided during preparation was useful, a number of essential issues were however never raised, or did not sufficiently prepare them to practice and everyday challenges, "…trainers presented an ideal system and not reality", "…if trainers had presented real life, all participants would have stood up and gone home".

When a child is placed in the family due to a crisis, foster parents often receive only very limited information, sometimes even lacking the background and the special needs of the child, including abuse history.

Although professional protocols require a two-week familiarisation period before placement, prospective foster parents and children cannot always go through this process due to urgency of placement for different reasons. Respondents agreed that the familiarisation phase has a greater significance with older children, especially with teenagers. Following the placement, integration of the child in the foster family is usually smooth, especially if the biological children of foster parents are well prepared and provide essential support for the foster child. According to respondents, patience and acceptance are the keys to successful integration. The acceptance of foster children in the local community depends on a wide range of issues, on the place and position of foster parents

in the local community and neighbourhood. Attitudes of professionals in health care and social services, kindergartens, schools are often not welcoming. This of course depends on the child's personality as well.

In case it is not against the best interests of the children, they have the right to keep contact with their biological parents. Children in 30 families meet their parents in the office of the local child welfare service. A little more than one fifth of the respondents said that the children regularly communicate with their biological parents via IT devices, while 11 respondents reported that biological parents visit their children in the foster family's home, and in 11 cases they take them for the weekend or holidays.

Thirty respondents have been fostering children for at least 5 years, only 7 respondents work as foster parents for less than 3 years. Two-third of the respondents have one or no biological child living in their household, while in eight cases two children, in six cases three children, and in 4 cases 4 children live within the foster family. Half of the respondents foster two or three children, in most of the cases foster children are siblings, while the others take care of four or five foster children. Only two responding families fostered seven children at the time of the research.

Judging their own role, some of the respondents emphasised a supporting, assisting role, focusing on the facilitation of the child's integration into society. Others emphasised an educative-caring role, aimed at preserving the child's health and supporting their development. Some of them think that their most important task is to take over the role of parents of origin (particularly if the child has no relatives who could take care of him/her), while some carers believe that all the above aspects are important part of their fostering identity. "I do fostering as a profession, but of course we cannot substitute biological parents. It's about doing our best to take care of them, educate them, to prepare them for adulthood."

For some of the foster parents, the overall objective is the reunification with biological parents, if possible, while for others it is to compensate for the child's disadvantages and to provide secure attachment. Facilitating independent living and anticipating appreciation from the community have also been raised as an important goal of their fostering. Almost all highlighted the representation of the child's rights as a major strength, even if it is not easy in a highly adversary environment. Another positive point is their capability to provide the child with a stable, loving atmosphere. Flexibility, consistency, representing a quality family model, ensuring a safe environment, the capability to set up a good relationship with families of origin and the ability to prepare the child for independent life were also mentioned.

Foster parents declared that they must be capable of solving all the problems occurring. However, some cases might be unmanageable, when one of the foster children endangers the others' psychological or physical health. Almost all of them had a related story.

The limited legal guardianship provided to foster parents is causing a lot of problems, when urgent decisions need to be made. In case of hospitalisation of the child or any incident occurring out of working hours requiring legal obligations, signatures or permissions, the legal guardian would be needed, often not accessible for different reasons. Many of the foster parents interviewed feel that their limited role is a sign of lack of trust

and appreciation, while the difficulties caused are very time- and energy-consuming. Although in principle guardians should visit the children in their homes at least once in three weeks, it hardly ever happens. On the other hand, all children have different guardians, which does not make it easy to meet all of them regularly.

The lack of opportunities to go for a holiday and have some time off for themselves was mentioned by foster parents as a serious problem, since there is no respite care or substitute parent available, despite of the theoretical opportunity based on their contract. The same applies in case the foster parents get getting ill.

Half of the foster parents interviewed feel left alone and lacking more guidance, vocational training and meeting opportunities, only 20% are participating in voluntarily organised self-help groups. The yearly compulsory twelve-hours vocational course is not enough to further develop their skills or learn more about specific questions.

All respondents agreed that the allowance provided to cover the costs of children's needs is much less than needed and they must contribute from their own resources. The administration on the money spent is very bureaucratic, while according to many foster parents: "The whole system is hypocritical, a large proportion of foster children live below the subsistence level, and everybody knows it. In case we cannot substitute the children are suffering."

There is also a common opinion that the regular maintenance of foster parents' own homes is not covered by the allowance, a substantial expenditure as well. Some of the respondents reported that due to many years of foster parenting, they used up all their savings, resulting in a very severe financial situation. Foster care benefit is also regarded as very low, given that foster families have enormous responsibilities and a 24/7 work schedule. A lot of respondents said this benefit is "ridiculously", "humiliatingly" low. They see this as an important sign of the lack of appreciation and despite of the public opinion about foster parents taking care of children to earn money, their opinion is that fostering is for those who feel the value of this activity "for the love and affection of the children in their care, in case the children are thriving, developing well, otherwise their success is not worth it".

3.3. Poland

Sixty-six non-related foster parents were included in the sample, leaving a large number of kinship carers and professional foster parents out of the analyses here. Almost a quarter of the carers have been foster parents for more than ten years, the other slightly less than a quarter between five and ten years, one fifth three or four years, one third between one and two years. One third of the families live in small settlements with under 2,000 inhabitants, 16% in towns accommodating between 5–20 thousand people, 13% between 20–100 thousand, nearly one quarter between 100–500 thousand, and 19% in cities larger than that, with only 1.3% living in the capital.

70% of the respondents are forming a couple, almost all of them married, as unmarried partners have no good chances to become foster parents, while the others are single women. Almost half of the foster parents have primary education (among them

two-third having some kind of vocational training), one third have got secondary education, and the rest college or university degree. Two-third of them are working, mostly full-time, 17% are retired.

Half of the foster parents did feel getting enough information on the child in their care. 46% of the children in foster care live together with their siblings, and half of all the children in the sample have got special needs.

The motivation to foster for 60% of the respondents was the desire to help children in need of care, for one fifth their own family situation. The community response was negative in only 8% of the cases, others were either positive, mixed or passive.

60% of the foster parents feel like a parent of the children, considering long-term care until the adulthood of the child, despite of the clear aim of temporary care provided in foster families to enable the reunification of the child with their own family or adoption as a permanent solution. 53% see their role in working together with specialists to serve the needs of the children, and only 17% to strengthen the opportunities to reunite the children with their families. Only one third of the families were mentioning the importance of the family of origin at all. 16% of the families wanted to have children in their families, not having their own, 17% needed the financial support provided, 19% having personal experiences, 25% knowing children in foster care and 13% liked the experience of acquainted foster families.

The foster families' most important aim is to ensure the safe development of the children (76%), and help them to become responsible adults (46%), providing positive and secure attachment (47%), meeting the special needs (22%), their own developments as foster parents (7%), returning the children to their families (15%).

As far as the satisfaction of the foster parents is concerned, helping the children in need is the most important for over two-third of them, followed by providing secure attachment and development. Half of them feel that they are doing something good, 41% detecting that children overcome their delayed development, and 13% for their own development, while some to fill the empty place in their families, after their grown-up children left.

The preparation for becoming foster parents has got many challenges, one third of them found it hard, and another third also not easy. They would have wished for a more realistic picture of fostering, more practical information on communication, building relationships with the children suffering from trauma and separation, about the contact and relationship with the families of origin. 36% participated in the PRIDE training, one third could not name it, while the rest in other pre-service programs. Almost half of the respondents meet the former group members sometimes. 13% participated at training sessions often, 30% never, and 10 % was not trained at all. Half of those receiving support mention vocational training, 7% self-help groups, 15% case conferences, or interdisciplinary teams and 7% supervision. More than two-third of those seeking support can rely on specialists in the family help centres, getting help from other foster families and their own relatives, one-third from friends, 16% from local services.

The desired help would include self-help groups, more financial and material resources, psychologists and therapy for the children, and regular supervision. The most useful kind of support is individual consultation with other foster parents and professionals

for over 80% of those responding, although 18% of them have issues they would not discuss with anybody.

As far as the local services are concerned, almost three-fourth of the respondents are satisfied with the cooperation with health professionals and local schools.

They see their foster family providing love (81%) and bonding (51%) to the children in their care, while meeting the individual needs (37%), access to specialist care (29%), their competences and expertise (29%), working as a team in the family (27%) and keeping contact with the family of origin (23%).

Concerning difficulties and challenges a third of the foster parents are struggling with the negative image of fostering, the need to keep contact with the biological families (27%), the behaviour of the child (18%), lack of rest, being overwhelmed (33%), financial difficulties (12%), specific needs of children (18%), lack of or limited access to specialist support (12%).

One fourth of the foster parents do not get any type of support or supervision, and half of them did not answer the questions related to the help and follow-up provided.

They would provide more information to foster families on how to support children experiencing trauma (36%), effective communication (33%), special needs (27%), positive discipline (26%), coping with the family of origin (21%), teamwork on planning (11%).

In almost half of the families (48%) children have regular contact with their families at least monthly, many of them more frequently and 21% have no contact at all. The families of origin meet the children in the foster care home (59%), have regular telephone, Internet contact (48%), meet in a family help centre (29%) at public places (21%), and one third of the children visit their families in their homes. A good indicator is, that 70% of the foster parents find the regular visits and bonding with the families of origin very important, and only 8% find it harmful for the child.

Less than half of the foster parents (45%) think they will be still foster parents in 5 years, 21% are planning to finish, others could not or did not want to answer.

3.4. Slovakia

The fifty respondents to the questionnaire were substitute and professional families from all over Slovakia, including nine families from settlements smaller than 2,000 inhabitants, and eleven from the capital city. Thirty foster families, five professional families, two mixed-function families, six kinship carers and seven foster families in family relation with the family of origin participated, making this sample different from those in the other three countries. More than half of the families take care of one child, 36% have got 2, and 12% 3 or more. 61% are married, 35% single women, one (2%) single man and one (2%) non-married couple. 90% of them have got at least secondary education.

The factors affecting their decision to become foster parents include the desire to help a child, prevention of placement in children's home, and earlier positive personal experience. The lack of an own child or the "empty nest" was also a factor contributing to

the decision made. 35 respondents had the primary reason to help a child and 15 because of their personal life situation.

The applicants found the preparation for the role quite difficult, many found it too long and would have required more practical information, knowledge on how to handle special needs, developmental delays, insecure attachment and information on the families of origin. 7% did not participate in pre-service training, while others took part in either accredited programs (39%) or a training provided by the office of social work and labour.

One third of the foster parents got information on the special needs of children placed in their families, 45% had been acquainted with the child placed there, while the rest did not get sufficient information of any kind on the child planned to be accommodated with them.

The vast majority of the families (85%) experienced mostly positive or mixed reactions from the wider environment, while 6% were suspicious and 9% got negative reflections. Two-third of them have been welcome by the health care professionals, 13% did not need specific help, while 22% could not get access to good quality services locally. Regarding schools and kindergartens, 70% had positive experiences, 12% were rejected and 18% had mixed responses. Many teachers were not knowledgeable or skilled in the field of developmental delays and special needs.

Relatives, friends and partners have been helping most of the carers, one third of them participating in self-help groups, some getting help from supervisors, NGO experts, local authorities or from the church. More than one third of the children need regular psychological support or other specialist visits.

62% of the children in the sample have no contact with their mothers, 22% have regular, 16% rare contacts only. 90% of them have not had any contact with their fathers, and very few had (8%) with grandparents. Despite these outcomes, the foster parents are aware of the importance of the contact with the family of origin.

The foster parents have various approaches to their own roles, 65% consider themselves parents of the child responsible for their upbringing until adulthood, while over one third of them see themselves as members of an expert team to take care of the child. Most of them (78%) see their role in providing permanency and secure attachment for the children, at the same time one quarter feel that their personal growth has a significant role and 16% aim to reunite the child with their family of origin.

One third of the foster parents focus on their own needs, while also doing good and be there for the children, helping a child in need, see the child developing and catching up. Over 70% mentioned love as a strength in the family, their ability to meet the needs of the children and 15% the cooperation with the family of origin.

Lack of opportunities to rest, the challenging behaviour of the children and their special needs, the insufficient support provided to the families and children, the low social status of substitute families, and the difficulties confronted in the contact with the biological families are among the problems listed.

Much higher financial support, more specialist help and supervision, more training and skill building would be needed according to the carers interviewed. Many of them mentioned the need for more help in working with trauma, effective communication at all levels and situations. They would like to learn more about ensuring the safety of children.

4. Conclusion

The above results provide important information on the substantial differences of the history and current system of child welfare and protection in four transition countries. Countries of the Central-Eastern European region are often seen as homogeneous or at least very similar to each other, while in fact both their history and their recent development in all areas including social policy, child protection policies and practices differ widely.

Despite the many differences it can be seen that there are important similarities both in terms of the characteristics of care provision and the needs of those taking care of the children. Several issues are mentioned as causing challenges, making the task of foster parents even more difficult, sometimes impossible to handle. While many of them are satisfied with their roles and activities in the life of children, the risk of burn-out, and the handling of unresolvable situations clearly require substantial improvements in all of the countries.

The needs are clearly articulated and provide sufficient information of those running the services and more broadly to policy and decision-makers. It has to be recognised that the participants taking part in the research were volunteers, and a larger sample of a representative survey would provide a more detailed and probably less positive picture. It also needs to be acknowledged that some issues were not raised or just mentioned, like the breakdown of placements, the strong resistance to and rejection of Roma and other children belonging to minorities, children with disabilities and no mention was made of LGBTQ related questions, among others.

The project should be considered as a first attempt to encourage further exploration of the foster care services in the countries covered and others, learning more about their functioning and opportunities to develop, just like the other elements of the child welfare and protection systems, involving children and parents, professionals working with families and children to understand their perspectives and needs.

The limitations and shortcomings notwithstanding, the main trends can be drawn. In case there is a strong commitment to implement a child rights-based approach, complex de-institutionalisation policies and practices based on the recommendations, guidelines, professional and legal requirements, family support, prevention, gatekeeping efforts have to be strengthened together with favourable conditions and help provided to kinship and foster parents accompanied by high quality local services to meet the needs of all children and families.

Child rights, the views of children taken into consideration in all matters affecting them in connection with their separation from their families and placement decisions, as well as their subjective well-being should be considered the most important elements of the desired changes. The incorporation of awareness and implementation of child rights in child welfare and protection is needed in both the pre- and in-service training of those working with children in alternative care. As children deprived of their own families are extremely vulnerable, their empowerment to be aware of their rights and to exercise them is an opportunity to ensure their well-being and opportunities to thrive.

Acknowledgement

References

Anghel, R., Herczog, M. & Dima, G. (2013). The challenge of reforming child protection in Eastern Europe: The cases of Hungary and Romania. *Psychosocial Intervention, 22*(3), 239–249. Online: https://doi.org/10.5093/in2013a27

Browne, K. D., Hamilton-Giacritsis, C. E., Johnson, R. & Chou, S. (2005). Young children in institutional care in Europe. *Early Childhood Matters, 105,* 15–18.

Diósi, Á. (1993). Cigány hivatásos nevelőszülők [Roma professional foster parents]. *Család, gyermek, ifjúság, 2*(6), 30–39.

Eurochild (2018). *Opening Doors for European Children: Hungary*. Online: www.openingdoors.eu/category/resources/publications/

Eurochild (2019). *New opportunities for investing in children 2019: Eurochild report on the European semester.* Online: https://shorturl.at/NgLPv

European Expert Group on the Transition from Institutional to Community-Based Care (2012, November). *Common European guidelines on the transition from institutional to community-based care*. Online: https://shorturl.at/iaACA

European Expert Group on the Transition from Institutional to Community-Based Care (2014, June). *Toolkit on the use of European Union funds for the transition from institutional to community based care* (Rev. ed.). Online: https://shorturl.at/OiERT

Fundamental Rights Agency (2023). *Mapping Child Protection Systems in the EU (27).* Online: https://shorturl.at/fwDPw

Goldman, P. S., Bakermans-Kranenburg, M. J., Bradford, B., Christopoulos, A., Ken, P. L. A., Cuthbert, C., Duchinsky, R., Fox, N. A., Grigoras, S., Gunnar, M. R., Ibrahim, R. W., Johnson, D., Kusumaningrum, S., Agastya, N. L. P. M., Mwangangi, F. M., Nelson, C. A., Ott, E. M., Reijman, S., van IJzendoorn, M. H., Zeanah, C. H., Zhang, Y. & Sonuga-Barke, E. J. S. (2020). Institutionalisation and deinstitutionalisation of children 2: Policy and practice recommendations for global, national, and local actors. *The Lancet Child & Adolescent Health, 4*(8), 606–633. Online: https://doi.org/10.1016/S2352-4642(20)30060-2

Herczog, M. (1997). Hungary. In M. Colton & W. Margaret (Eds.), *The World of Foster Care. An International Sourcebook on Foster Family Care Systems* (pp. 107–121). Arena.

Hungarian Central Statistical Office (2024). *Summary Tables (STADAT).* Online: www.ksh.hu/stadat_eng

Kaasbøll, J., Lassemo, E., Paulsen, V., Melby, L. & Osborg, S. O. (2019). Foster parents' needs, perceptions and satisfaction with foster parent training: A systematic literature review. *Children and Youth Services Review, 101,* 33–41. Online: https://doi.org/10.1016/j.childyouth.2019.03.041

Knuiman, S., Rijk, C. H., Hoksbergen, R. A. & van Baar, A. L. (2015). Children without parental care in Poland: Foster care, institutionalization and adoption. *International Social Work, 58*(1), 142–152. Online: https://doi.org/10.1177/0020872812473138

Kolankiewicz, M. (2006). Zapiski o instytucjonalnej opiece nad dziećmi [Remarks on the institutional care of children]. *Dziecko krzywdzone: Teoria. Badania. Praktyka, 5*(4), 6–35.

Łuczyński, A. (2007). Rodziny zastępcze – ich rola i zadania w systemie opieki całkowitej [Foster families – Their role and tasks in the care system]. In J. Kuźma (Ed.), *Opieka i wychowanie dzieci sierocych w Polsce* [Care and upbringing of orphan children in Poland] (pp. 67–97). Krakowskie Towarzystwo Edukacyjne.

Lumos (2018). *Investing in Children. The case for diverting Czech government finances away from institutions towards families and communities.* Online: https://tinyurl.com/mwvt9pyj

Moravkova, S. (2018). *Identification of the benefits of care about children in professional families in the Slovak Republic.* NORDSCI Conference on Social Sciences. Online: https://doi.org/10.32008/NORDSCI2018/B1/V1/52

Muhari, J. (2024, May 3). Annyi elhagyott baba vár nevelőszülőre, hogy már a csecsemőosztályt tehermentesítő otthon is megtelt a miskolci kórházban [There are so many abandoned children waiting for foster parents that even the infant home replacing the postnatal ward is full]. *Népszava.* Online: https://shorturl.at/pJpSe

National Assembly (2024, June 10). A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény módosítása [Draft Amendment of Act XXXI of 1997 on the protection of children and guardianship administration]. Online: www.parlament.hu/irom42/08560/08560.pdf

Neagoe, A., Neag, D. L. M. & Lucheș, D. (2019). Reasons to care: Personal motivation as a key factor in the practice of the professional foster carer in Romania. *PLOS ONE, 14*(9). Online: https://doi.org/10.1371/journal.pone.0222716

OHCHR Expert Consultation on the Rights of the Child (2021). Online: https://tinyurl.com/bddtpujd

Ruszkowska, M. & Lovašová, S. (2023). The foster care system in Poland and Slovakia. A comparative analysis/study. *Rozprawy Spoleczne, 17*(1), 227–238. Online: https://doi.org/10.29316/rs/175191

Schmidt, V. & Bailey, J. D. (2014). Institutionalization of Children in the Czech Republic: A Case of Path Dependency. *The Journal of Sociology & Social Welfare, 41*(1), 53–75. Online: https://doi.org/10.15453/0191-5096.3833

Stelmaszuk, Z. W. (2002). Residential Care in Poland: Past, Present and Future. *International Journal of Child and Family Welfare, 5*(3), 102–111.

SzocOkos (2023, April 12). *Nevelőszülők* [Foster parents]. Online: https://tamogatoweb.hu/neveloszulok-2/

The Budapest Beacon (2018, March 28). EMMI sued for taking away too many Roma children from their families due to poverty. *The Budapest Beacon.* Online: https://tinyurl.com/2j9ptfbb

The League of Human Rights (2017, March 31). Czech Ministers at Loggerheads over Infant Homes & Foster Care. *Liberties.* Online: https://tinyurl.com/4tr5m5n4

Tobis, D. (2000). *Moving from residential institutions to community-based social services in Central and Eastern Europe and the former Soviet Union.* World Bank.

Truhlárová, Z. & Levická, T. (2012). Facilities for children needing immediate assistance – controversial institutions intended for substitute childcare in the Czech Republic. *Social Work in Ukraine: Theory and Practice, 2,* 132–147.

UN Committee on the Rights of the Child (2021). *Day of General Discussion, Children's Rights and Alternative Care, Outcome Report.* Online: https://shorturl.at/gRXFf

UN General Assembly (2020). Resolution adopted by the General Assembly on 18 December 2019. Rights of the Child. Online: https://undocs.org/en/A/RES/74/133

UNICEF (2012). *Moving forward: Implementing the guidelines for the alternative care of children.* Online: https://shorturl.at/dq3OK

UNICEF (2013). *Fifteen years of de-institutionalization reforms in Europe and Central Asia: Key results achieved for children and remaining challenges.* Online: https://shorturl.at/sXWIn

UNICEF & Eurochild (2021). *Better data for better child protection systems in Europe: Mapping how data on children in alternative care are collected, analysed and published across 28 European countries.* DataCare Project Technical Report. Online: https://shorturl.at/T5uzY

Vecchiato, T., Maluccio, A. N. & Canali, C. (Eds.) (2002). *Evaluation in Child and Family Services. Comparative Client and Program Perspectives.* De Gruyter.

Whenan, R., Oxlad, M. & Lushington, K. (2009). Factors associated with foster carer well-being, satisfaction and intention to continue providing out-of-home care. *Children and Youth Services Review, 31*(7), 752–760. Online: https://doi.org/10.1016/j.childyouth.2009.02.001

Contents