ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Fascicolo Speciale n. 4 (2025)

Charting the Course Towards a New Legal Framework for Smart Cities

CERIDAP **Fascicolo Speciale 4 (2025)**

DIRETTORE RESPONSABILE: Prof.ssa Diana-Urania Galetta
Iscritta con delibera 16.06.2020 nell'Elenco Speciale dei direttori responsabili di periodici o riviste a carattere scientifico annesso all'Albo dei Giornalisti della Lombardia

Inserita nell'elenco delle Riviste scientifiche di classe A con Delibera ANVUR n. 147/2023

Rivista indicizzata nella Directory of Open Access Journals e in SCOPUS.

- Prof. Mary Crock (University of Sydney, Australia)
- Prof. José Luís da Cruz Villaça (Universidade de Lisboa, Portugal e Corte di Giustizia dell'EU, Lussemburgo)
- Prof. Pedro Cruz Villalón (Universidad Autónoma de Madrid, España)
- Prof.ssa Daria de Pretis (Università degli Studi di Trento e Corte costituzionale, Italia)
- Prof. Rosario Ferrara (Università degli Studi di Torino, Italia)
- Prof. Guido Greco (Università degli Studi di Milano, Italia)
- Prof. Constance Grewe (Université de Strasbourg, France)
- Prof. Ian Harden (University of Sheffield, UK)
- Prof. Carol Harlow (London School of Economics)
- Prof. Herwig Hofmann (Université du Luxembourg)
- Prof. Martin Ibler (Universität Konstanz)
- Prof.ssa Julia Iliopoulos-Strangas (Università Nazionale e Kapodistriana di Atene, Grecia)
- Prof.ssa Maria Immordino (Università degli Studi di Palermo, Italia)
- Prof. Vittorio Italia (Università degli Studi di Milano, Italia) †
- Prof. Jean-Paul Jacqué (Université de Strasbourg, France et Service juridique du Conseil de l'UE, Bruxelles)
- Prof. Irena Lipowicz (Università Cardinale Stefan Wyszyński di Varsavia, Polonia)
- Prof. Mario G. Losano (Università degli Studi di Milano e del Piemonte orientale, Italia)
- Prof. Roberto Mastroianni (Università degli Studi di Napoli, Italia e Tribunale dell'UE, Lussemburgo)
- Prof. Jacqueline Morand-Deviller (Université Paris 1 Panthéon-Sorbonne, France)
- Prof. Bruno Nascimbene (Università degli Studi di Milano, Italia)
- Prof. Luke Nottage (University of Sydney, Australia)
- Prof. Angelika Nussberger (Universität Köln, Deutschland e Corte Europea dei diritti dell'uomo, Strasbourg, France)
- Prof. Giorgio Orsoni (Università Ca' Foscari Venezia, Italia)
- Pres. Alessandro Pajno (Presidente emerito del Consiglio di Stato)
- Prof. Vasco Pereira da Silva (Universidade de Lisboa, Portugal)

CERIDAP è una rivista ad accesso libero sul sito ceridap.eu, aggiornata on-line quotidianamente e fascicolata trimestralmente. Alla fine di ogni trimestre gli articoli riprodotti nel sito sono tutti pubblicati nel fascicolo del trimestre di riferimento.

CERIDAP è la Rivista nata nel 2020 dall'iniziativa del Direttore dell'omonimo Centro di Ricerca Interdisciplinare sul Diritto delle Amministrazioni Pubbliche dell'Università degli Studi di Milano per un'azione amministrativa più efficiente e più imparziale, anche in attuazione del principio digital first. La Rivista CERIDAP, pur indipendente dall'omonimo Centro, è la sede principale in cui vengono pubblicate le ricerche svolte in seno al Centro stesso e si è avvalsa sin da principio della collaborazione, all'interno del suo Comitato di Direzione, di un gruppo di studiosi dell'area giuspubblicistica provenienti da vari Atenei, sia italiani che stranieri, che ne condividono l'impostazione di fondo e la filosofia ispiratrice.

Obiettivo della Rivista CERIDAP è di fornire un contributo di analisi, approfondimento e proposta avente come focus principale le Pubbliche Amministrazioni: intese sia nella loro dimensione istituzionale, organizzativa e di attività, che nella loro dimensione procedurale. E con una naturale apertura prospettica anche al diritto comparato, europeo ed

internazionale nonché alla discussione interdisciplinare che è favorita dalla presenza, nel suo Comitato scientifico, di autorevoli studiosi provenienti da prestigiosi Atenei di tutto il Mondo.

Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito, e agli autori non sono imposti costi di elaborazione e pubblicazione. La Rivista si uniforma agli standard internazionali definiti dal Committe on Publication Ethics (COPE), e fa proprie le relative linee guida.

CERIDAP è interessata a pubblicare contributi relativi a tutti gli ambiti scientifico-disciplinari che sono riferibili al c.d. Diritto Pubblico, inteso nella sua accezione più ampia e che ricomprende anche aree di analisi al confine fra la scienza giuridica e le scienze c.d. politologiche. CERIDAP è inoltre aperta all'approccio tipico dell'analisi economica del diritto. Per questa ragione si è dotata di un "Comitato dei Revisori" che include anche esperti provenienti da aree di expertise diverse da quella del Diritto Pubblico tradizionale (costituzionale ed amministrativo).

Per la citazione dei contributi presenti in questo fascicolo di CERIDAP, si consiglia di utilizzare la forma di seguito esemplificata: N. Cognome, *Titolo del contributo*, in *CERIDAP*, 2025, speciale n. 4/2025, p. 35 ss.

Per l'invio di contributi destinati alla pubblicazione: ceridap.eu/rivista/invio-contributi

INDICE SOMMARIO

ARTICOLI

HANNO COLLABORATO A QUESTO NUMERO:

GABRIELA BLAHOUDKOVÁ, Ricercatore di Diritto Amministrativo nell'Università Karlova di Praga, Repubblica Ceca.

MARC-OLIVIER BUSSLINGER, Dottorando di Ricerca in Diritto Pubblico nell'Università di Ginevra, Svizzera.

JAKUB HANDRLICA, Professore Ordinario di Diritto Amministrativo nell'Università "Karlova" di Praga.

ALESSIA MONICA, Ricercatore (RTT) di Diritto Amministrativo nell'Università degli Studi di Milano, abilitata alle funzioni di Professore di II fascia.

MARIANNA NOVOTNÁ, Professore Associato di Diritto Civile nell'Università di Trnava, Slovacchia.

RICHARD POMAHAČ, Professore Ordinario di Diritto Amministrativo e Scienze Amministrative nell'Università Karlova di Praga, Repubblica Ceca.

JULIO PONCE SOLÉ, Professore Ordinario di Diritto Amministrativo nell'Università di Barcellona, Spagna.

LEONARDO SCUTO, Dottore di Ricerca in Diritto Pubblico, Internazionale ed Europeo (curriculum Diritto amministrativo) nell'Università degli Studi di Milano e Avvocato nel foro di Milano.

LILIIA SERHIICHUK, Dottoranda di Ricerca in Diritto Pubblico nell'Università Karlova di Praga, Repubblica Ceca.

VLADIMÍR SHARP, Assistant Professor nell'Università Karlova di Praga, Repubblica Ceca.

VERONIKA ZORIČÁKOVÁ, Assistant Professor nell'Università di Trnava, Slovacchia.

Introduction

The articles published in the Special Issue n.4/2025 of CERIDAP are revised and expanded versions of papers presented at the *Chartering the course towards a new legal framework for Smart Cities* round table, which took place at the Law Faculty of the Charles University in Prague, Czech Republic, on 11th October 2024. This round table was organised jointly by the Department of Administrative Law at the Law Faculty of the Charles University and the Interdisciplinary Research Centre for Public Administration (CERIDAP) at the Law Faculty of the University of Milan.

This Special Issue aims to contribute to the emerging legal scholarship on smart cities. A smart city is a place where traditional networks and services are made more efficient through digital solutions, benefiting its inhabitants and businesses. The concept of a smart city goes beyond using digital technologies to use resources better and reduce emissions. It means more intelligent urban transport networks (See J. Ponce, *Artificial Intelligence, Urban planning and the (Right to) Housing in Smart cities*), upgraded water supply and waste disposal facilities, and more efficient ways to light and heat buildings. It also means a more interactive and responsive city administration, safer public spaces together with *a new perception of privacy* (See., R. Pomahač*, Privacy in Smart Cities)* with the needs of an ageing population. These cities of the future have recently been studied from various viewpoints, including urbanism, digitalisation, energy security and transition (See J. Handrlica and G. Blahoudková*, Microreactors for powering data centres, miniaturisation of technologies and the paradigm shift in nuclear law)* and transport (See, M. Novotná and V. Zoričáková*, Deployment of AI in public transport in smart cities as a challenge for tort law).* The articles published in this Special Issue aim to address the phenomenon of smart cities from a legal point of view, addressing both issues in public and private law *with sustainability goals serving as a guiding framework*. However, it is important to underline that the concept of smart cities is not yet precisely defined in EU law or the majority of national legislations of Member States, despite the fact that the phenomenon of smart cities is present in Europe. Their development is largely based on administrative cooperation, with local governments experimenting a newly significant role. (See, M. O. Busslinger*, Smart cities in Switzerland: local autonomy versus centralisation).*

Academicians with backgrounds in different legal jurisdictions wrote the articles published in this Special Issue. However, as technological innovations and progress are omnipresent, all authors are addressing the same phenomenon. At the same time, this Special Issue contains papers written by authors from the Czech Republic (See, V. Sharp, *Smart administrative punishment: a slippery slope of automated decision-making and its economic incentives in public law*,) Italy (See, A. Monica and L. Scuto, *Energy communities for smart cities: a challenge for EU administrative law in light of the Italian perspective)*, Switzerland, Slovakia, Spain and Ukraine (See, L. Serhiichuk*, Digitalisation of public administration under martial law in Ukraine and the case of Smart City Kyiv)*, that is, from countries traditionally classified as "Western", "Central" and "Eastern" Europe. Nevertheless, the concept of smart cities is

not constrained by state boundaries. Despite the existence of disparities in legal frameworks, all authors embody the same concept. As such, this Special Issue of CERIDAP is also to be interpreted as the authors' contribution to the concept of Europe as a technology hub, which has united various legal and regulatory traditions.
The articles published in this Special Issue of CERIDAP were written under the umbrella of the 4EU+ project, *Chartering the course towards a new legal framework for Smart Cities*, and within the Jean Monnet Module 101175226 – *Public Administrations in the EU Energy Policies and Communities* (PAEPeC).

Introduzione

I contributi pubblicati nel Fascicolo Speciale n. 4/2025 di CERIDAP costituiscono una rielaborazione rivista e ampliata degli interventi presentati alla tavola rotonda "*Chartering the course towards a new legal framework for Smart Cities"*, tenutasi l'11 ottobre 2024 presso la Facoltà di Giurisprudenza della Charles University di Praga, Repubblica Ceca. La tavola rotonda è stata organizzata congiuntamente dal Dipartimento di Diritto Amministrativo della Facoltà di Giurisprudenza della Charles University di Praga e dal Centro di Ricerca Interdisciplinare sul Diritto delle Amministrazioni Pubbliche (CERIDAP) della Facoltà di Giurisprudenza dell'Università degli Studi di Milano.
Questo Fascicolo Speciale mira a contribuire alla nascente letteratura giuridica sulle città intelligenti. Una città intelligente è un luogo in cui le reti e i servizi tradizionali sono resi più efficienti attraverso soluzioni digitali, a vantaggio dei suoi abitanti e delle imprese. Il concetto di città intelligente va oltre l'uso delle tecnologie digitali per utilizzare meglio le risorse e ridurre le emissioni. Significa reti di trasporto urbano più intelligenti (cfr. J. Ponce, *Artificial Intelligence, Urban planning and the (Right to) Housing in Smart cities*), strutture di approvvigionamento idrico e smaltimento dei rifiuti migliorate e metodi più efficienti per illuminare e riscaldare gli edifici. Significa anche un'Amministrazione comunale più interattiva e reattiva, spazi pubblici più sicuri e «*una nuova percezione della privacy*» (cfr. R. Pomahač*, Privacy in Smart Cities)*, tenendo conto delle esigenze di una popolazione che invecchia. Queste città del futuro sono state recentemente studiate da vari punti di vista, tra cui l'urbanistica, la digitalizzazione, la sicurezza energetica e la transizione (cfr. J. Handrlica e G. Blahoudková*, Microreattori per l'alimentazione dei centri dati, miniaturizzazione delle tecnologie e cambiamento di paradigma nel diritto nucleare)* e i trasporti (cfr. M. Novotná e V. Zoričáková*, L'impiego dell'IA nei trasporti pubblici nelle città intelligenti come sfida per il diritto civile)*. I contributi pubblicati in questo Fascicolo Speciale mirano ad affrontare il fenomeno delle città intelligenti da un punto di vista giuridico, affrontando sia le questioni di diritto pubblico che quelle di diritto privato*,* «*con gli obiettivi di sostenibilità come quadro di riferimento*». Detto questo, va ricordato che, sebbene il fenomeno delle città intelligenti esista in Europa, non esiste ancora una definizione giuridica precisa di questo concetto, né nel diritto dell'Unione europea né nella maggior parte delle legislazioni nazionali degli Stati membri. Il loro sviluppo si basa in gran parte sulla cooperazione amministrativa,

con gli enti locali che sperimentano un ruolo nuovo e significativo (cfr. M. O. Busslinger*, Smart cities in Switzerland: local autonomy versus centralisation)*.

Gli articoli pubblicati in questo numero speciale sono stati redatti da accademici con formazioni giuridiche diverse. Tuttavia, poiché le innovazioni e i progressi tecnologici sono onnipresenti, tutti gli Autori affrontano lo stesso fenomeno. Allo stesso tempo, questo numero speciale contiene articoli scritti da autori provenienti dalla Repubblica Ceca (cfr. V. Sharp, *Smart administrative punishment: a slippery slope of automated decision-making and its economic incentives in public law*), Italia (cfr. A. Monica e L. Scuto, *Comunità energetiche per le città intelligenti: una sfida per il diritto amministrativo dell'UE alla luce della prospettiva italiana)*, Svizzera, Slovacchia, Spagna e Ucraina (cfr. L. Serhiichuk*, Digitalizzazione della pubblica amministrazione sotto la legge marziale in Ucraina e il caso della Smart City Kyiv)*, ovvero paesi tradizionalmente classificati come Europa "occidentale", "centrale" e "orientale". Il fatto è, tuttavia, che il concetto di città intelligenti non rispetta i confini statali. Tutti gli autori riflettono lo stesso concetto, nonostante le differenze nei quadri giuridici ancora esistenti. Pertanto, questo Fascicolo Speciale di CERIDAP va inteso anche come il contributo degli Autori all'idea di un'Europa come polo tecnologico, che unisce tradizioni giuridiche e normative diverse.

Gli articoli pubblicati in questo Fascicolo Speciale di CERIDAP sono stati redatti nell'ambito del progetto 4EU+ "*Chartering the course towards a new legal framework for Smart Cities*" ("*Tracciare la rotta verso un nuovo quadro giuridico per le città intelligenti*") e del modulo Jean Monnet 101175226 – "*Public Administrations in the EU Energy Policies and Communities*" (PAEPeC, "*Amministrazioni pubbliche nelle politiche energetiche e nelle comunità dell'UE*").

Milan-Prague/Milano-Praga, June 2025/Giugno 2025
The Editors/I curatori: Jakub Handrlica, Alessia Monica, Leonardo Scuto.

Smart cities in Switzerland: local autonomy versus centralisation

Marc-Olivier Busslinger

DOI: 10.13130/2723-9195/2025-2-31

Le città intelligenti in Svizzera fanno parte della tendenza alla trasformazione digitale delle amministrazioni pubbliche. Questi processi sono guidati dai Comuni. Quasi tutti gli aspetti della governance pubblica e dei servizi pubblici possono essere considerati parte di questi sforzi di digitalizzazione. Poiché i programmi per le Smart City sono progettati da autorità guidate democraticamente, e poiché questi programmi sono orientati agli obiettivi e incentrati sui clienti, si sostiene, nel presente contributo, che l'autonomia locale sia necessaria per una "buona" implementazione di una Smart City. Tuttavia, l'implementazione di processi digitali è per lo più giustificata da guadagni di efficienza ed efficacia. Sia la tecnologia come strumento, sia il ragionamento per l'implementazione di queste tecnologie potrebbero portare a processi di centralizzazione e, paradossalmente, a una perdita di autonomia locale. L'interesse delle autorità cantonali e federali a trasformare digitalmente l'amministrazione pubblica sta già portando alla perdita di autonomia dei comuni in numerosi settori. Sosteniamo che questa tensione, tra autonomia locale e ricerca di servizi pubblici efficaci ed efficienti, sia già presente nella Costituzione federale e che il sistema manchi di garanzie costituzionali. Sebbene siano necessarie ulteriori ricerche per meglio coniare le possibili soluzioni, il presente scritto vuole suggerire alcune soluzioni che potrebbero aiutare a preservare l'autonomia locale.

Smart cities in Switzerland are a part of the trend of digital transformation of public administration. These processes are led by local authorities in the municipalities (communes). Almost all aspects of public governance and public services can be considered as part of these digitisation efforts. Since Smart city programmes are designed by democratically led authorities, and because these programmes are goal-oriented and customer-centred in nature, we argue that local autonomy is necessary for a "good" implementation of a Smart city. However, the implementation of digital processes is mostly justified by gains of efficiency and effectiveness. Both technology as a

tool, and the reasoning for implementing technologies might lead to centralisation processes and paradoxically, to a loss of local autonomy. The interests of cantonal and federal authorities to digitally transform public administration are already on the way to strip away the autonomy of municipalities in numerous areas. We argue that this tension, between local autonomy and a search for effective and efficient public services, is already present in the federal constitution and that the system lacks constitutional safeguards. Although further research is needed to better coin possible solutions, we suggest a few solutions that could help preserve local autonomy.

1. Smart cities in Switzerland

1.1. The Federal level

There is no unified definition of smart cities in Switzerland[1]. The Swiss Confederation in their strategy "digital Switzerland" in 2018 wished to encourage the implementation of «*intelligent cities and municipalities*»[2]. The goal was in particular to «*have real "intelligent data" at all levels of government*» at the service of smart cities[3]. This objective sadly vanished from later strategies on the federal level[4]. The scope of the "digital Switzerland strategy" broadened to lead to a «*sustainable digital transformation that is ecologically, economically and socially responsible*»[5]. This strategy is mandatory only for the federal authorities but is conceived as a source of inspiration for other levels of the federal state[6]. The cooperation between the central state, the cantons and the cities and municipalities, is also a key part of the Swiss digital public services strategy[7]. In both strategies, the need for a data driven policymaking and a

capacity development are present[8]. These objectives are then implemented in "projects" that the Digital Public Services Switzerland organisation is promoting and coordinating, some of which are oriented toward municipalities[9] and could be described, in a broader sense as being part of Smart City's initiatives. For example, one of the projects tried to encourage the «*[c]reation, distribution and delivery of municipal services to any cantonal portal and municipal websites*»[10].
In parallel and apparently with little links with the precedent organisation, the Swiss Confederation is funding the programme "Swiss Energy" that develops a "Smart city program"[11]. For them, «*[a] Smart City offers its residents a high quality of life with minimal consumption of resources, thanks to networking, closer collaboration, participation and innovation*»[12] they support local projects from a broad nature[13], ranging from citizens' participation[14] to the implementation of nudging to encourage the installation of solar panels[15]. In other documents they explain that they chose not to have a fixed definition of what a smart city should be to leave the decision to the local authorities[16].
Beside the federal authorities' actions, specialised organisations are also active on a federal level to sustain the development of smart cities in Switzerland. They have adopted their own definition of what a smart city is or should be. The "Smart city hub Switzerland"[17], an association of cities and interested enterprises[18] uses a broader definition: «*Smart City stands for holistic, future-oriented development concepts that aim to make cities more efficient, technologically advanced, greener and more socially inclusive*»[19]. Contrary to the federal state's program, the focuses seem here less about collaboration between actors and the gain in energetic efficiency and more about the area of public action or the different programmes that makes a smart city. The SwissDigital association for communication networks[20] is also supporting smart city initiatives. Although they also consider that no unified definition has made consensus, they describe the phenomenon as trying to achieve a «*more efficient city capable of adapting constantly as part of an overall concept based on digital technology*»[21]. The interconnection being a key piece of infrastructure to transfer and interpret the data collected, data which is at the centre of the cities of the future[22].

1.2. The regional level

The cantons don't seem to be particularly active in the field of smart cities. Some cantons have decided to name their cantonal strategies "Smart"[23]. If all cantons have adopted an eGovernment strategy or a digitisation strategy for their public services[24], some of them even have a common strategy shared between cantons and municipalities. For those that don't have a common strategy, the cantonal strategy generally contains a chapter about the collaboration with the municipalities, few strategies integrate the terminology of "smart city" explicitly[25]. The canton of Geneva offers one of the few definitions of the term of Smart cities we could really find in an official document in Switzerland: «*Smart city refers to a city that uses information and communication technologies, particularly sensors, to improve the quality of life of its inhabitants and increase energy efficiency*»[26].

1.3. The local level

It is difficult to determine the exact number of smart cities present in Switzerland[27]. We argue that the relatively vague definition of smart city[28] is partly responsible for this analytic difficulty. Some definitions suggested in the literature could almost encompass any "modern" local administration programme, for example smart city: «*Urban development that integrates information and communication technology (ICT) and Internet of things (IoT) technology in a secure fashion to manage a city's assets, deliver city services effectively, efficiently, and equitably. Smart city uses information and communications technology (ICT) to enhance liveability, workability, and sustainability*»[29]. We argue that the inclusion of a programme into a Smart city ideal might be a question of threshold as well as of political will or even of analytical approach[30]. If we consider the implementation of one eGovernment project as a proof for a city to be future-oriented and thus to be on the path to become a smart city, every municipality in Switzerland might fit into this denomination[31].

In 2019, only one third of the municipalities and cities of Switzerland had a smart city strategy in place while another third of the municipalities and cities were

developing one[32]. Numerous smart city strategies and projects are developed and publicised by the organizations active around smart cities[33] or by the municipalities themselves[34]. Depending on the municipality, almost every area of public services and public policy making might have been digitised. The smart city wheel[35] encourages municipalities to digitise and apply the smart city concept to very diverse areas[36].

2. Swiss smart cities are a product of, and in need of local autonomy

However we choose to define them, Smart cities in Switzerland are a product of their communities[37]. The projects are implemented by authorities that try to answer to local problems to answer to the needs of their citizens[38]. The projects currently implemented are very different, as they touch every aspect of the authorities' responsibility. Even more, similar problems aren't always resolved in the same manner[39], and very different problems might also sometimes have similar solutions[40].

Since cities aren't identical, because of their geography, their history, their demographics, their infrastructure, they face different challenges that a "one fit's all solution" will most likely not be able to solve. This consideration is also present from the idea of Smart cities as processes that should be both "goal oriented"[41] and "customer oriented"[42] and based on "citizen participation"[43].

Moreover, the municipalities in the Swiss tradition are conceived and built as democratic vessels, possessing their own elected officials, own legislative body and their own sets of direct or semi-direct democratic tools[44]. These tools are used relatively often, and the communities are used to be consulted to choose between different priorities, they will fix different sets of preferences in the way public policy should be conducted[45], and which technological solution should be implemented.

The projects attached to Smart cities in Switzerland today are mainly a product of the local autonomy, granted to the municipalities to regulate their own projects and priorities[46]. The federal and cantonal programmes supporting smart cities are mainly active to support and to fund local initiatives[47]. In order to have as many projects falling under the scope of smart cities, the organisations

promoting smart cities programme present these as an “holistic approach” with a very broad list of aspects that can be included in these projects[48].
Although more research is needed on the impact of the federal and cantonal state’s strategies on the municipality’s actions[49], Smart cities programmes don’t operate in a vacuum. The municipalities are tasked with executing cantonal and federal laws and see their autonomy limited in multiple domains[50].

3. The pursuit of technology is a vector for centralisation

3.1 The expectations from the authorities towards technology

If we consider the reasons that justify the implementation of smart cities strategies, we see that most programmes are in search of effectiveness and efficiency of public policy through the collection of data and the delivery of public services[51].
To increase the effectiveness[52] of public policy it is necessary to increase data collected in the communities, to adopt a “data based” policy making[53]. This is made possible with the augmentation of the number of captors and indicators on physical infrastructure as well as the increase in the amount of data processed electronically by eGovernment forms and platforms[54]. It is also necessary to improve the public services provided, which these technologies are providing through an easier and quicker bureaucratic experience electronically, but also by automating certain tasks in the physical as well as the digital sphere[55]. The rapid development of AI in the public sector[56] seems to promise an increase in the automation of administrative tasks as a mean to provide even quicker and “better” service. In addition, these technologies allow for a better communication with the citizens and should provide more transparency into the administration’s inner functions[57].
If efficiency, as a search for the best cost-benefit solution[58], is central, then cost reduction and saving might be a key factor in the choice of a technology[59]. The development of platforms and software being very expensive, the authorities might be encouraged to reuse existing software, they might even prefer to adapt their processes rather than to develop or adapt existing software to their need[60].

On a larger scale, there might be a push for the adoption of unified solutions rather than decentralised ones. See for example this call for «*the introduction of a standardised legal form for binding cooperative between municipalities and cantons simplify collaboration and speed up the implementation of joint digital projects*»[61].

3.2 The consequences these expectations might have on local autonomy

We argue that the implementation of informatics and of technologies as a mean to gather information and data and to provide for public service is a vector of centralisation. Both a philosophical point of view and a practical necessity will lead to a shift in power over the technology that could result in a loss of autonomy for the municipalities and cities. In this sense, these pursuits, of effectiveness and efficiency of public services, present some risks for the local autonomy. Indeed, some municipality "fear for their autonomy and are reluctant to participate in common projects"[62].

The quest for more and better data, as a mean for decision making at all levels of government[63], means that the cantonal and federal authorities might in the future need the data created by the smart cities[64]. To be used at a higher level of government, this data will likely need to be centralised. In general, for the data to be useful, to be able to interpret the data and to use it, it needs to be structured and presented in an organised way, it needs to be connected to the systems of the supervising entity[65]. The national data management programme (NaDB)[66] will most probably bring the most changes in the matter in the future as it envisions to «*ensure simpler and more efficient management of government data through the multiple use of data. To this end, the public authorities concerned must make uniform use of data catalogues and metadata*»[67].

This has for consequence that standards, in the structure of data as well as for the different steps in their internal processes and the technical conception of the software and platforms might need to be followed by the municipalities when they decide to informative a public policy. The Federal government and the representatives of the cantonal administrations decided to consider that norms developed by eCH, the Swiss eGovernment standardisation association[68], as

«*generally declared to be binding*» in the conception of eGovernment systems[69]. These standards are generally considered necessary to attain the goals of digitisation as an overreaching process[70], but they might also limit the autonomy of each municipality taken individually to organise and to create their own digital platforms and services.

The search for effectiveness and efficiency also means that the cantonal or federal authorities might be tempted to force the municipalities to adapt their processes to collect the data they need[71]. This push for the adoption of common software might then be explained by the need to limit the public spending needed for such developments[72].

The digitisation of some processes, which can now be considered part of what makes smart cities, follow such a path. In 1999, most municipalities had local inhabitants' registers[73], which justified the federal government to adopt a law to uniformise the data collection toward the federal statistical agency[74], thus limiting their autonomy. The Federal government has begun work discussing a project to centralise and uniformise the registry for underground pipes partly based on data collected and managed by the municipalities[75], although debates about the need for centralisation might hinder the development of this project[76]. The risk also exists that, once a solution is developed and tested, the higher levels of government would want to have influence on this new piece of technology, to be able to use it at their level, in their environment, to serve their goals. The example of traffic lights is in this sense very exemplative, traffic lights have the capacity to be put on a network to react intelligently with one another or even to be controlled remotely[77]. Some municipalities have seen mandates from a regional authority to give away their regulatory power to serve broader interests[78].

4. The tension between Technology and local autonomy is also present in the constitution

The search for an efficient and effective government and public policy action is present in the federal constitution (art. 43a al. 5 Cst.[79]) that «*[s]tate tasks must be fulfilled economically and in accordance with demand*»[80]. The Constitution also provides for an evaluation of the effectiveness and effectivity of the federal

legislation (art. 170 Cst.)[81].

On the other hand, you have notably[82] the need of communal autonomy as part of a democratic system, which is also enshrined in the Federal Constitution at the article 50 al. 1 Cst.[83]. This article states that the autonomy of municipalities and cities protected «*in accordance with cantonal law*». The tribunals and the doctrines consider this protection not to be absolute, the doctrinal opinions are divided on the possibility for the cantons to totally suppress municipalities or to transform them into mere decentralised administrative entities[84]. To know if a municipality is autonomous, it is «*sufficient to determine whether it is free to make choices under its own responsibility, and according to options that it defines itself*»[85].

For the implementation of its legislation, the Federal state should, as much as possible, rely on the cantons and delegate them the implementation of said policies (art. 46 al. 1 Cst.)[86]. The cantons are, in turn, free to delegate certain tasks to the municipalities in their cantonal laws[87]. The communal autonomy protected by the federal constitution is in this sense mainly used to forbid the cantons to exceed their own powers or to misuse their statutory powers as defined by cantonal laws[88].

The Confederation is merely supposed to «*take account in its activities of the possible consequences for the municipalities*» (art. 50 al. 2 Cst.) as well as the «*special position of the cities and urban areas*» (art. 50 al. 3 Cst.). These provisions have been interpreted in several ways by the authorities. First, the organisation representing the municipalities are systematically consulted before a law is presented to the federal assembly[89]. Secondly, special organisations uniting municipalities, cantons and the Confederation were created to spark dialog between these instances, in particular in order to support the implementation of "urban areas"[90]. Thirdly, the Confederation adopted internal guidelines concerning the contact between the Confederation and the municipalities[91] in which the Confederation decided that «*[d]irect contacts between the Confederation and the municipalities are of an exceptional nature. Exceptions are justified where federal legislation directly entrusts the municipalities with implementation tasks, or when measures taken by the Confederation affect certain municipalities in particular. The cantons must be informed of such direct contacts*»[92].

The municipalities have the right to defend their autonomy in front of courts[93], but only the cantonal norms are open to a full review[94]. The same isn't true in for federal laws that are "protected" by the Constitution (art. 190 Cst.) that forces the federal court to apply federal and international laws[95]. On a federal level, the arbitration between constitutional norms, between effectiveness, efficiency and local autonomy, is in the hands of Parliament. The judicial review is limited and when cases arise where a choice is left to the court, they favour a consistent interpretation of the constitution[96].
Since many centralisation processes are led by the federal government, we argue that the risk posed by the digital transformation to local autonomy might not be sufficiently protected.

5. Outlook and possible solutions

If the risk exist that the implementation of Smart cities programmes will participate in a broader tendency towards centralisation, we are of the opinion that this situation is not a necessity. The implementation of said technologies and the normative apparatus allowing these implementations will have the most impact on the future of local autonomy, and thus on the future of semi-direct democracy at a local level. We hope to see further research in this field to evaluate and promote effective provisions in a highly interconnected world. Here are a few positive outlooks on the possible ways to solve this tension between technology-based centralisation and local autonomy.
First, in accordance with the Constitutional responsibility to respect the municipality's autonomy, there is a need for a stronger political will, at all levels of Government, to defend the local autonomy. Since the discourse surrounding smart cities and the entire digitisation from the state also contain a push for more local participation and democracy[97], we consider that both the cantons and the Confederation should be proactive to guarantee for such participation to exist. It means that certain decisions need to stay "open" for public debate. Future regulations on a cantonal or federal level should contain provisions to such processes, a certain degree of "liberty". When deciding at a higher level of government to "force" the interconnection of systems or processes, we argue that it is also necessary to determine explicitly the level of freedom guaranteed for the

lower levels. It is in this sense necessary to voluntarily decide not to regulate the entirety of the process and of the technological solutions to leave a margin of choice to the "lower" political bodies for them to exercise their democratic rights. Moreover, the specialised organisations accompanying public authority's digitalisation effort should support these efforts from the political authorities and should restrain the advocacy for centralising solutions.

As discussed in the first part of this paper, there is to date, no unified definition of what a Smart city is, nor real limits to what it can encompass. We fear that defining Smart cities in a legal text on the federal or on the cantonal level could have adverse effects on the autonomy of municipalities. Such a definition would necessarily limit the autonomy and creativity of the municipalities in their implementation of technologies. Allowing Municipalities to decide which project is or isn't part of their Smart city programmes and how they want to prioritise their projects is in our view a competency that should stay at a Municipal level. More than a definition of Smart cities, regulations should focus on directing principles for the digital transformation as a phenomenon that includes Smart cities. These principles should in our opinion be oriented towards "digital sovereignty"[98] and resilience of all levels of government in the sense that they should participate in safeguarding the local autonomy and define interdependencies, collaboration and coordination between the different state's actors to maintain their innovation and adaptability capacities.

In this sense, changes on a constitutional and legal level are in our opinion warranted to define specific provisions for local autonomy in the digital transformation processes. Innovations in terms of judicial review powers granted to the federal courts could help arbitrate the conflict between the different constitutional principles. The question of democratic and participation rights granted to citizens should also be examined more closely. Indeed, Smart cities would profit to have official legitimate democratic support early in the process. Moreover, when intergovernmental authorities are created to lead specific projects, democratic rights and provisions for democratic procedures should in our opinion be implemented for the system to stay "customer oriented".

1. Notably, Termdat, the terminology database of the Federal Administration has no entry for "smart city" and it's declinations.

2. The Swiss official terminology is “commune” or “Gemeinde” in German. In order to simplify the wording, we chose to use “municipality” to describe local authorities; *Stratégie «Suisse numérique»*, of the 5 September 2018, FF 2018 6007, p. 6024 (free translation from the author).
3. *Idem*.
4. See for example the *Stratégie Suisse numérique 2025*, of the 13 December 2024, FF 2025 31.
5. *Idem*., art. 1, p. 2.
6. *Ibidem*.
7. *Stratégie Administration numérique suisse 2024–2027*, of the 8 Décember 2023, FF 2024 45, p. 21.
8. In particular through the implementation of the “digital first principle”, see art. 3 FF 2025 31, p. 4 and art. 3 FF 2024 45, p. 7.
9. https://www.digital-public-services-switzerland.ch/en/implementation/projects.
10. https://www.digital-public-services-switzerland.ch/en/implementation/agenda-dvs/digital-channel-between-the-public-and-the-administration.
11. https://www.local-energy.swiss/fr/programme/smart-city#/
12. Free translation from their website: https://www.local-energy.swiss/fr/programme/smart-city/was-ist-eine-smart-city.html#/.
13. They publish a database of projects on their website, see https://www.local-energy.swiss/fr/arbeitsbereich/projektdatenbank.html#/q/tPr=63ce32ac-e51e-4538-b100-3383bec20beb.
14. https://www.local-energy.swiss/fr/beispiele/projekt/Projekte/2024/ParticipoNs.html#/.
15. https://www.local-energy.swiss/fr/beispiele/projekt/Projekte/2024/solarize-schaffhausen.html#/
16. J. Musiolik et. al., *Smart City - Guide de mise en œuvre des initiatives Smart City en Suisse*, SuisseEnergie pour les communes, 2019, p. 9.
17. https://www.smartcityhub.ch.
18. https://www.smartcityhub.ch/members.159en.html.
19. https://www.smartcityhub.ch/goals.14en.html.
20. https://www.suissedigital.ch.
21. P. Stennhauser, *Smart city – une introduction*, SuisseDigital et HWZ, 2018 , see *Que signifie vraimaiment le terme «Smart»?*, p. 6 (16), free translation from the author.
22. *Idem*, p. 8 (18).
23. For example in canton Aarau, *SmartAargau: Strategie Digitale Transformation*, 2019; the canton of Geneva also has a “smart Geneva” programme in parallel to their “digital transformation” program, see https://www.ge.ch/dossier/smart-city.
24. For an overview and the links to each canton’s strategies, see https://www.administration-numerique-suisse.ch/fr/publications/sondages/012023-strategies-de-numerisation-des-cantons.

25. Canton Basel-city decided to use the definition smart cities to define the expectations from their digital transformation strategy, see https://digital-basel.ch/grundsaetze/.
26. Rapport, *une politique numérique pour Genève*, Conseil d'état, Genève, 20.06.2018, p. 84 ss. - free translation from the author.
27. In 2022, only 87 municipalities accepted to answer a survey on the matter on the 2121 municipalities of Switzerland as of jan. 2025, see B. Sütterlin et al., *Swiss Smart City Survey 2022 - Final Report*, Winterthur, ZHAW, 2023, p. 2.
28. See for example the very different meanings of what a smart city can be in J.C. Augusto (ed.), *Handbook of Smart Cities,* Springer, Cham, 2021, https://doi.org/10.1007/978-3-030-69698-6.
29. P. James et al., *Smart cities: Fundamental Concepts* in *Handbook of Smart Cities,* Springer, Cham, 2021, p. 30.
30. Some author prefer to describe local projects as part of a more global digitalisation movement, see T. Mettler, *The Road to Digital and Smart Government in Switzerland* in A. Ladner et al. éd., *Swiss Public Administration: Making the State Work Successfully*, Palgrave Macmillan Cham, 2019, p. 183 ss., https://doi.org/10.1007/978-3-319-92381-9_10.
31. We couldn't find statistics about the availability of municipal services online, but we are yet to find a municipality without a website. In 2022, about 70% of the user interrogated communicated via e-mails with their municipal authorities while ~60% used electronic platforms, see M. Buess, *Nationale E-Government-Studie 2022*, Bern, p. 20.
32. S. Wiederkehr et al., *Stakeholderanalyse Smart City Switzerland*, AWK, Bern, 2019, p. 4.
33. See for example the repository proposed by the smart cities compass: https://www.swiss-smart-city-compass.com/en/cities-regions.html or the list proposed by the smart city hub: https://www.smartcityhub.ch/fact_sheets.506en.html.
34. For cities that are pushing smart city programs without really being referenced on a broader level, see for example https://smart.pully.ch/en/home/.
35. https://www.smartcityhub.ch/smart_city_wheel.120en.html.
36. A large variety of projects are digitized some more "trivial" than others, for example some municipalities decided to implement process to allow the mobile buying of pool access https://smart.pully.ch/en/projects/id-1428-e-ticket/.
37. For a study of Swiss municipalities goals see S. Wiederkehr et al., cit., p. 4.
38. For an analytic study see F. Wäspi, et al., *On the Way to Smarter Cities: What Goals and Values Swiss Municipalities Prioritize*, in M. Janssen et al., *Electronic Government*, EGOV 2022, Lecture Notes in Computer Science, vol. 13391, Springer, Cham, https://doi.org/10.1007/978-3-031-15086-9_29.
39. In order to allow for more dialog between the citizens and the authorities, the cities of Lenzburg, St-Gallen, Luzern have decided to implement different systems of participation: see the search for participation (in German) on the smart-city compass, https://www.swiss-smart-city-compass.com/de/use-cases.html?tx_solr%5Bq%5D=partizipation.

40. For example, the installation of sensor to regulate public lights might be interesting for factors ranging from ecology to safety concern.
41. In a Swiss context, see S. Haller, *Monitoring-Konzept für Gemeinden*, v. 2.0, Innoville, Bern 2021, in particular p. 4 ss.
42. eGovernment projects follow in this sense the principles developed by New Public Management principles, see J. Chappelet, *The New Model of Swiss Public Management* in A. Ladner et al. (ed.), *Swiss Public Administration*, 2019*,* p. 169 ss.
43. In a Swiss context, see for example J. Musiolik et al., *Smart City - Guide de mise en œuvre des initiatives Smart City en Suisse*, cit., p. 33.
44. For an in depth study of the different democratic tools implemented by the municipalities see for example S. Micotti, M. Bützer, *La démocratie communale en Suisse : vue générale, institutions et expériences dans les villes 1990-2000*, Genève, 2003*,* in particular p. 31 ss.
45. For a global overview of the influence of local autonomy for Swiss municipalities, see K.W. Debela, *Local governance in Switzerland: Adequate municipal autonomy cum intergovernmental cooperation?,* in *Cogent Social Sciences, 6:1,1763889, DOI: 10.1080/23311886.2020.1763889.*
46. Protected by art. 50 Cst., see *infra*.
47. The swiss energy smart city programme is funding different type of projects, for example the "innovative city project" grants up to 40% of the price of a project led by certain municipalities, see https://www.local-energy.swiss/fr/programme/projektfoerderung/fortschrittliche.html#.
48. The smart cities wheel and their very large scope of action are in this sense exemplative, see for example https://www.smartcityhub.ch/smart_city_wheel.120en.html.
49. Among the few exceptions, see A. Marmier, *The Impact of Data Governance on OGD Publication – An Ethnographic Odyssey*, in Loni Hagen et al. (ed), *dg.o 2022: The 23st Annual International Conference on Digital Government Research,* 2022, https://doi.org/10.1145/3543434.3543438.
50. For a rapid overview of the repartition of tasks between the tree level of government, see A. Ladner, *The Organization and Provision of Public Services,* in A. Ladner et al. (ed.), 2019, p. 26.
51. The same reasoning apply in every digital transformation programme *Res Publica Digitalis*, Digital Switzerland, Berne, 2024, p. 6.
52. A. Flückiger, *(Re)faire la loi: traité de légistique à l'ère du droit souple*, Berne, Stämpfli, 2019, p. 462.
53. V.B. Clarissa, *Public Sector Data Openness in the Crafting of the data-driven Society: The Co-constitutive role of regulation and innovation*, Thesis Université de Lausanne, 2024, p. 113.
54. *Idem* p. 22 ss.
55. *Stratégie Administration numérique suisse 2024–2027*, FF 2024 24, p. 18.
56. On the federal level see *Conseil federal, «Intelligence artificielle» – lignes directrices pour la Confédération,* 2020, and the specialised website : https://cnai.swiss/fr/.

57. On the federal level, see *Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2019 à 2023 (Stratégie Open government data, OGD)* du 30 novembre 2018, FF 2019 855, p. 856.
58. A. Flückiger, *(Re)faire la loi: traité de légistique à l'ère du droit souple*, cit., p. 465.
59. J. Musiolik et al., *Smart City - Guide de mise en œuvre des initiatives Smart City en Suiss Smart City - Guide de mise en œuvre des initiatives Smart City en Suisse*, cit., p. 36.
60. The specialised organisations recommend such practices, J. Musiolik et al., *Smart City - Guide de mise en œuvre des initiatives Smart City en Suisse*, cit., p. 17 which explain the repositories of experience provided online, see for example https://www.zhaw.ch/index.php?id=11283.
61. Res Publica Digitalis, cit., p. 7, free translation from the author. The study references a cantonal position advocating for mandatory standards and infrastructure : Kantonsrat St.Gallen, *Digitale Transformation schweizweit mit gebündelten Kräften angehen,* vom 2 april 2024 KSG 41.21.01.
62. Res Publica Digitalis, cit., p. 49.
63. V.B. Clarissa, *Public Sector Data Openness in the Crafting of the data-driven Society: The Co-constitutive role of regulation and innovation*, cit., p. 22 ss.
64. It is in particular true for geo-data and sensors data, see for example the project MODI about mobility data: https://www.bav.admin.ch/bav/fr/home/themes-generaux/modi.html. The law proposal submitted to public consultation creates a new obligation for municipalities to transfer their geo-data (art. 8 al. 3) see *Procédure de consultation du 2 février 2022 - Loi fédérale concernant l'infrastructure de données sur la mobilité* (AP-LIDMo)*,* FF 2022 294.
65. On a theoretical level, see for example R. Sandoval Almazán et al. *Building Digital Government: Strategies Principles and Practices*, Springer, Cham, 2017, DOI 10.1007/978-3-319-60348-3, p. 60.
66. Programme of the federal statistical office: https://www.bfs.admin.ch/bfs/fr/home/nadb/nadb.html.
67. *Programme national de gestion des données: En route pour l'avenir avec la gestion nationale des données*, Berne, Repport of the 23 août 2023, p. 3.
68. https://ech.ch/fr.
69. Art. 1.4 al. 2 *Convention-cadre de droit public concernant la collaboration en matière de cyberadministration en Suisse 2020*, of 20 December 2019, FF 2019 8257.
70. For example, see Res Publica Digitalis, cit., p. 63.
71. The Federal Government proposed at some point to give itself the power to «*impose the use of online administrative services*» (art. 12 AP-LMeta) and norms (art. 13 AP-LMeta) to cantons and other entities tasked to apply federal laws, *Avant-projet de Loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (AP-LMETA)* abandoned before the project was submitted to Parliament; see *Message concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités*, of 4 march 2022, FF 2022 804, p. 44 s.

72. FF 2022 804, p. 48.
73. *Message concernant l'harmonisation de registres officiels de personnes*, of the 23 November 2005, FF 2006 439, p. 450.
74. *Federal Act on the Harmonisation of the Register of Residents and of other Official Registers of Persons (Register Harmonisation Act, RHA)*, of 23 June 2006 RS 431.02.
75. See the report referenced by the FF 2024 69 for the opening of a public consultation, *Modification de la loi sur la géoinformation - Introduction d'un cadastre des conduites Suisse (CCCH),* 12.2023, in particular p. 13 ss.
76. The Federal Assembly is currently debating a previous change to the same law about the geology of the country and the constitutionality of such a project is highly debated. See object 23.060, modification to the GeoInformation Law, in particular the intervention of M. Kolly Nicolas about the constitutionality of the change in BO 2024 N 1728.
77. C. Rhodes, S. Djahel, *TRADER: Traffic Light Phases Aware Driving for Reduced Traffic Congestion in Smart Cities, International Smart Cities Conference (ISC2)*, 2017, DOI**:** 10.1109/ISC2.2017.8090783.
78. For a local example, in the commune of Morges, canton of Vaud, see the credit proposal N° 44/11.20 of the 26.10.2020 for the implementation of captors and traffic control central that was refused by the legislative body in part for fear to loose it's autonomy, see the point of M. Thuler in procès-verbal du 31.03.2021, N° 44/ 2016-2021, p. 1179.
79. Constitution of the Swiss confederation of the 18 April 1999 (Cst.), RS 101.
80. For a commentary see F. Bellanger art. 43a Cst., n. 34 ss., in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, Helbing Lichtenhahn, Bâle, 2021.
81. For a commentary see A. Lienhard, F.M. Locher, art. 170 BV, in B. Waldmann et al., *BSK Bundesverfassung*, St-Gallen, 2015, in particular n. 18 ss., for the evaluation of public policies.
82. Other problems can also be caused by a strong orientation towards efficiency and effectiveness see T. Mettler, *Transformation digitale,* in N. Soguel et al. (ed.), *Comprendre et concevoir l'administration publique – Le modèle IDHEAP*, EPFL Press, Lausanne, pp. 210 s.
83. For a commentary see: A. Thévenaz, art. 50 Cst., n. 20, in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, cit.
84. A. Thévenaz, art. 50 Cst, n. 13, and references in note 48, in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, cit.
85. G. Malinverni et al., *Droit constitutionnel Suisse - volume 1 L'État*, 4e ed., Stämpfli, Berne, 2021, pp. 279, free translation from the author.
86. See O. Bigler-de Mooij, art. 46 Cst. n. 31 ss in particular, in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, cit.
87. Malinverni et al., *Droit constitutionnel Suisse - volume 1 L'État*, cit., pp. 293 ss.
88. A. Thévenaz, art. 50 Cst., n. 15 ss., in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, cit.
89. Art. 7 al. 1 *Lignes directrices à l'attention de l'administration fédérale concernant la*

collaboration entre la Confédération, les cantons et les communes, 16 octobre 2002, FF 2002 7795.

90. The tripartite conference was instituted to encourage the collaboration between these three instances (art. 1 let. a CT) and "participates in the development of a common policy for agglomerations" (art. 1 let. c CT). *Convention entre la Confédération, les cantons, les villes et les communes sur la Conférence tripartite (CT)* du 28 octobre 2020, RS 701.
91. FF 2002 7795.
92. *Idem*, art. 8 al. 3, FF 2002 7795 p. 7797, free translation.
93. G. Malinverni et al., *Droit constitutionnel Suisse - volume 1 L'État*, cit., p. 2213 ss.
94. G. Malinverni et al., *Droit constitutionnel Suisse - volume 1 L'État*, cit., p. 299 ss.
95. For a commentary see for example V. Martenet, art. 190 Cst, in V. Martenet, J. Dubey (ed.), *Commentaire Romand – Constution fédérale*, cit.
96. For a commentary on constitutional jurisdiction in Switzerland, see for example M. Hottelier, *La justice constitutionnelle en Suisse*, in *Fédéralisme Régionalisme,* Volume 17, 2017, *Les juridictions constitutionnelles suprêmes dans les États fédéraux : créatures et créateurs de fédéralisme*, DOI: 10.25518/1374-3864.1718, chapter 4.3.
97. See for a "global orientation" the study *Res Publica Digitalis*, cit., p. 56. For a more specific study of the phenomenon, see for example Timon Sengewald et al., *Influence of Digital Open Innovation Platforms on Power Differentials within Municipalities* in SIGMIS-CPR '24: 2024 *Computers and People Research Conference,* Murfreesboro TN USA, 2024, https://doi.org/10.1145/3632634.3655877.
98. For an analysis on all level of government, see for example Y. Benhamou et al., *Souveraineté numérique: étude pluridisciplinaire pour la Suisse,* Geneva, 2023, https://archive-ouverte.unige.ch//unige:168718.

Microreactors for powering data centres in smart cities, miniaturisation of technologies and the paradigm shift in nuclear law

Jakub Handrlica, Gabriela Blahoudková

DOI: 10.13130/2723-9195/2025-2-11

L'utilizzo dei dati e il traffico internet globale hanno registrato una crescita esponenziale a partire dalla metà degli anni Duemila e si prevede che la tendenza continui e addirittura acceleri a causa dell'ampia adozione dell'intelligenza artificiale. La domanda totale di energia a livello mondiale per i data center supera oggi il consumo della maggior parte delle economie e gli stessi emettono circa il 2%-4% delle emissioni globali di gas serra. Per soddisfare questa domanda, i progettisti di data center devono considerare non solo gli aspetti di convenienza economica, ma anche la sostenibilità, la sicurezza dell'approvvigionamento e l'impatto sociale. A questo proposito, si è recentemente discusso dei microreattori nucleari come di una soluzione per l'alimentazione dei data center completa, priva di emissioni e basata sulle fonti rinnovabili, poiché in futuro saranno in grado di fornire energia pulita e affidabile a costi contenuti e di creare posti di lavoro qualificati. I microreattori nucleari, che saranno probabilmente impiegati nel prossimo decennio, presentano diverse sfide significative che li differenziano dagli impianti nucleari già in funzione. Il loro carattere miniaturizzato implica una notevole riduzione dei rischi. Inoltre, possono servire come strumento per il decentramento dell'alimentazione e possono essere collocati proprio nel centro degli insediamenti urbani. Questo articolo sostiene che la prospettiva di impiego dei microreattori rappresenta una parte integrante di un discorso molto più ampio sull'emergere delle città intelligenti. Allo stesso tempo, gli autori sostengono che la futura diffusione dei microreattori implica un notevole cambiamento di paradigma verso una moderna legge nucleare.

Data usage and global internet traffic have experienced exponential growth since the mid-2000s, and the trend is expected to continue and even accelerate due to the wide adoption of artificial intelligence. The total global energy demand for data centres

now exceeds the consumption of most economies, and they emit around 2% to 4% of global greenhouse gas emissions. To meet this demand, data centre planners must consider not only the affordability aspects but also sustainability, supply security, and social impact. In this respect, nuclear microreactors have been recently discussed as a comprehensive, emission-free and renewable-led solution for powering the data centres in smart cities, as in the future, they will be capable of supplying cost-effective, clean and reliable energy and creating skilled jobs. Nuclear microreactors, which will likely be deployed in the next decade, demonstrate several significant challenges that differentiate them from nuclear installations that have been in operation. From the authors' perspective, their miniature character implies a considerable decrease in risks. Also, they may serve as a tool for the decentralisation of power supply and can be located right in the very centre of urban settlements. Lastly, microreactors will be very easily transportable by land, sea, or air. This article argues that the future deployment of microreactors does imply a considerable paradigm shift towards a modern nuclear law. This is very similar to the space sector, where space law has been needed to address the gradual deployment of small satellites and nanosatellites (CubeSats or NanoSats); also, nuclear law is currently being triggered to establish new rules, reflecting this paradigm shift arising from miniaturisation.

1. Introduction

The smart cities of tomorrow will need far more than just power for homes and businesses. As cities increasingly rely on electric vehicles, the need for reliable, fast-charging infrastructure will grow. Clean power will be needed to charge fleets of electric buses, trams, taxis, personal cars and autonomous transport systems. They will also require energy for edge computing, real-time monitoring, and the myriads of Internet of Things (IoT) devices that will keep the city running smoothly[2]. Similarly, data centres, which are critical to the functioning of smart cities, will consume vast amounts of energy. These centres must be

online 24/7 to process the data flowing in from traffic cameras, air quality sensors and public safety systems. The rise of artificial intelligence (AI) has recently also contributed to a massive build-out of new data centres. In this respect, it has been argued that data centres will soon become the backbone of the newly emerging smart cities[3]. Still, power consumption has become one of the key bottlenecks to further expansion[4]. In this respect, nuclear power has been currently identified as an option that is seriously considered for deployment in the forthcoming decade[5].

On 7th March 2023, the Swedish data centre operator Bahnhof announced a plan to launch a nuclear microreactor to power its future data centre. The prospective microreactor is envisaged to be operated in the industrial site of the Hjorthagen area of Stockholm. It will provide electricity for a new data centre, 30.000 households, and heat for homes and offices[6]. For the time being, Bahnhof operates seven data centres in various cities in Sweden. The company is well known for its underground data centre, Pionen White Mountains, in central Stockholm. It is built in a former government nuclear bunker and has backup power provided by diesel engines recovered from submarines. The fact is, however, that the recently announced plan of the Swedish data centre operator Bahnhof does not represent the only existing endeavour aiming at powering a data centre with a nuclear microreactor. In July 2024, the US-based nuclear start-up Nano Nuclear Energy Inc. announced it had signed a Memorandum of Understanding (MoU) with Blockfusion Ventures, an affiliate of crypto mine firm Blockfusion USA, Inc. Under this MoU, Nano Nuclear will explore the potential integration of its microreactor technologies with Blockfusion's remote data centre in Niagara Falls, New York[7]. In October 2024, Google signed an agreement with nuclear startup Kairos Power to build seven microreactors that will supply electricity to its data centres until 2035[8]. Another MoU was adopted in December 2024 between Nano Nuclear Energy and Digihost Technology to advance the transition to carbon-free energy for Digihost's high-tech operations, including AI-driven data centres and digital asset colocation programmes[9].

The prospective deployment of microreactors to power future data centres has already attracted considerable attention from scholars who are dealing with technologies, smart cities, and energy transition[10]. At the same time, there is a common understanding that a robust legal and regulatory framework must

accompany any future deployment of microreactors[11]. This article argues that the prospective deployment of microreactors also implies a considerable paradigm shift in law. While classical nuclear law had to address the potential risks arising from large nuclear reactors, future nuclear law will need to reflect the specifics arising from the miniaturisation[12] of nuclear technologies.

Having said this, the need to address challenges arising from technology miniaturisation does not occur exclusively in the nuclear sector. A very similar process is currently ongoing in the field of space technologies. Here, the miniaturisation of satellites has opened the door to missions that a larger satellite could not accomplish, such as providing constellations for low data rate communications, using formations to gather data from multiple points, in-orbit inspection of larger satellites, etc[13]. The increased commercial interest in small satellites has recently triggered the adoption of national space acts, addressing their licencing, registration and liability issues[14]. In Europe, such national space acts have been recently adopted in Portugal (2019), the Grand Duchy of Luxembourg (2020) and Slovenia (2022). In 2023, both Cyprus and the Principality of Liechtenstein adopted their space acts. Legislative activities towards adopting national space acts are currently pending in the Federal Republic of Germany, Latvia and Spain. France recently undertook the update of its national legal framework, including its Law of 2008 on space activities. On 28 June 2024, French lawmakers released a decree and two orders on authorisation and technical regulations applicable to space activities[15]. In Italy, a draft of a national act on Provisions for the Space Economy was submitted to the Parliament on 10 September 2024[16]. At the same time, the adoption of an EU Space Law is pending at the European Union level[17].

This article aims to argue that similar legislative developments regarding microreactors may be expected in the forthcoming decade. The Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2024, which President Joe Biden signed on 9 July 2024, represents the first demonstration of these developments, which will continue in the future.

2. A fleet of microreactors is on the horizon!

The announcements on the prospective deployment of microreactors to power

data centres must be understood in the context of the recent boom of commercial interest in advanced nuclear technologies. Very recently, the 2024 edition of the OECD/NEA Small Modular Reactor Dashboard presented 56 various projects[18] of small modular reactors (SMRs) that are currently under development worldwide. Both public and private institutions in different countries[19] are actively participating in efforts to bring SMR technology to fruition within this decade. As a class of reactors, SMRs are defined by their smaller size[20]. However, there is considerable variety within this class of reactors; they vary by power output, temperature output, technology and fuel cycle. Several SMRs are based on existing commercially deployed light water technologies. In contrast, others are based on advanced design concepts, offering a range of sizes (from 1 MWe to over 300 MWe) and a range of temperatures (from 285°C to more than 850°C) to meet the specific energy needs of hard-to-abate industrial sectors[21]. Having said this, one must bear in mind that the primary aim of SMR development is not to replace the nuclear power plants in operation already but to provide an advanced and alternative source of energy in the future[22]. Existing projects target varied outputs and different applications, such as electricity, hybrid energy systems, heating, hydrogen production, water desalinisation and steam for industrial applications. For the time being, the following benefits of a prospective deployment of SMRs have been identified: Firstly, SMRs are expected to play an essential and increasingly important role in supporting net-zero targets[23]. Secondly, given their smaller footprint, SMRs can be sited in locations not suitable for larger nuclear power plants. Prefabricated units of SMRs can be manufactured and then shipped and installed on-site, making them more affordable to build. In this respect, SMRs offer savings in cost and construction time, and they can be deployed incrementally to match increasing energy demand[24]. Also, SMRs can be installed into an existing grid or remotely off-grid as a function of their smaller electrical output, providing low-carbon power for industry and the population. Lastly, proposed SMR designs are generally more straightforward, and the safety concept for SMRs often relies more on passive systems, such as low power and operating pressure. This means that in such cases, no human intervention or external power or force is required to shut down systems[25].

Microreactors represent a specific type of these newly emerging advanced nuclear

technologies[26]. The International Atomic Energy Agency (IAEA) defines them as very small reactors with power levels anticipated generally ranging from less than 1 MWe to 30 MWe[27]. The US Department of Energy (DOE) defines[28] microreactors by using three distinctive features:

Microreactors are factory-fabricated: All components of a microreactor are fully assembled in a factory and shipped to the location.

Microreactors are transportable: Smaller unit designs will make microreactors very transportable by truck, shipping vessel, plane or railcar.

Microreactors are self-adjusting: These advanced nuclear technologies won't require many specialised operators and would utilise passive safety systems that prevent any potential for overheating or reactor meltdown.

At the end of 2024, thirteen microreactor projects worldwide were under various stages of development worldwide[29]. Many of these projects reflect the exponential growth of data usage and global internet traffic, which is expected to continue and even accelerate due to the wide adoption of AI. To meet this demand, data centre planners consider not only the affordability aspects but also sustainability, supply security, and social impact. In this respect, microreactors have been recently discussed as a comprehensive, emission-free and renewable-led solution for powering data centres in the future. In this respect, Westinghouse is currently developing its eVinci™ microreactor, which combines microreactor's innovative design with 60+ years of commercial nuclear design and engineering, creating a cost-competitive and resilient source of power with superior reliability and minimal maintenance. Its small size allows for transportability and rapid, on-site deployment in contrast to plants requiring large amounts of construction[30]. In September 2024, Westinghouse submitted its eVinci™ Microreactor Preliminary Safety Design Report to the US Department of Energy (DOE). Westinghouse announced that the move advances the eVinci™ microreactor's testing for future use on the commercial market, including data centres[31]. Other microreactors for powering data centres are currently being developed by the NuScale Power Corporation (NuScale) and by Nano Nuclear Energy Inc[32]. Having said this, one must bear in mind that the prospective applications of microreactors are not limited to data centres powering. It has been envisaged that microreactors can power remote urban settlements and mining operations, produce hydrogen, or provide power on a space basis. Also, they are planned to

be operated by universities and research institutions for scientific purposes[33].
For the time being, microreactor deployment is envisaged in the forthcoming decade. For example, the MoU between Google and the nuclear startup Kairos Power foresees that the first microreactor will power Google's data centre by 2030, and the following six installations will be completed by 2035[34]. The microreactor, which is subject to the MoU adopted between Nano Nuclear Energy and Digihost Technology, is envisaged to be operated in 2031. Also, Bahnhof foresees the launch of a microreactor to power the future data centre at the Hjorthagen area of Stockholm within the next decade.
Having said this, one may expect that a brand-new type of advanced nuclear technology will be deployed in the forthcoming decade. However, any such deployment must be accompanied by the establishment of a transparent and predictable legal framework.

3. Miniaturisation as a trigger for a paradigm shift in nuclear law

The existing legal framework for the peaceful uses of nuclear energy has been established to address risks potentially arising from large (conventional) nuclear reactors. However, microreactors, which will probably be deployed in the next decade, demonstrate several significant challenges that differentiate them from installations that have been in operation in the US and Europe until now[35]. The feature of miniaturisation implies the main challenges arising from the prospective deployment of microreactors[36]. These challenges can be outlined as follows.

3.1. Reduction of size & risks

Microreactors are the most minor type of SMRs[37]. They are 100 to 1000 times smaller than conventional nuclear reactors and range in capacity from 1 to 30 MWe, compared to 30 to 300 MWe for SMRs. The fact is, however, that microreactors do not represent a mere miniaturisation of large nuclear reactors. One of the significant differences between large reactors and microreactors is that microreactors won't require many specialised operators and will utilise passive safety systems that prevent any potential for overheating or reactor meltdown

and subsequent radioactive release into the environment. Thus, the prospective risks arising from microreactors will be considerably lower in the future than those arising from conventional reactors[38].

However, nuclear law has been designed to address risks arising from conventional nuclear reactors[39]. To address these risks, legal mechanisms have been established in the fields of nuclear safety and nuclear liability. While nuclear safety aims to minimise the risk of a radioactive release into the environment, nuclear liability schemes are intended to govern cases involving nuclear damage. In the field of nuclear safety, the Convention on Nuclear Safety provides[40] that its Contracting Parties must adopt a system of licensing regarding nuclear installations and prohibit the operation of a nuclear installation without a licence[41]. Further, the Convention confers licencing of nuclear installations to the hands of national regulatory authorities. In the Euratom Community, these requirements have been reiterated in by the Directive 2009/71/Euratom[42]. With respect to this requirement, rules for licencing procedures have been provided by the national legislation and implemented by national regulatory authorities. However, these licencing procedures have been designed for large reactors rather than for microreactors. Thus, national legal frameworks provide for rather complex and lengthy procedures that match the level of risk implicated by conventional reactors. Facing the prospective deployment of microreactors in the forthcoming decade, countries interested in hosting these technologies must adopt rules of licencing that will fully reflect the potential number of operated installations and the considerably reduced risks arising from the operation of such installations[43].

The feature of miniaturisation also has significant implications for the regime of nuclear liability. The existing regime of liability for nuclear damages was designed in the 1960s to reflect potential transboundary risks arising from then-existing nuclear technologies. Two international liability regimes – the Paris-Brussels regime and the Viennese regime – provide for liability rules, which need to be further transferred into the national legislation. Having said this, one must bear in mind that the existing regime of nuclear liability has been tailor-made for risks arising from large reactors[44]. In the existing nuclear liability regime, the operator of the nuclear installation is exclusively liable for any damages that may occur because of an incident in the respective installation. National legislation provides

for mandatory insurance for this liability and requires the operator to maintain it in a certain amount during the whole operation of the licenced installation. While these amounts for compulsory insurance have been determined with respect to the risks potentially arising from large reactors, any future deployment of microreactors will require reconsideration of these amounts[45].

3.2. Decentralisation

Prospective deployment of microreactors will significantly contribute to the decentralisation of power supply, dramatically changing the landscape of power supply. In the past, large reactors have represented a tool for centralising power supply from a few power generation centres in the territory of the state. Microreactors will enrich this landscape of power generation. Large reactors will cease to represent the only source of nuclear power in the state. Nuclear power will be generated from a much higher number of centres, which will be distributed according to the delivery needs of the respective urban communities, industrial regions, etc[46].

The fact is, however, that the deployment of microreactors can change the current paradigms in nuclear law enforcement in different ways. Apart from the requirement for licencing of nuclear installations, the Convention on Nuclear Safety also provides that national legislative and regulatory framework must establish and maintain «*a system of regulatory inspection and assessment of nuclear installations to ascertain compliance with applicable regulations and the terms of licences*»[47]. Under the safety scheme of the Convention, both regulatory inspections and assessments of nuclear installations must be realised by national regulatory authorities. In this respect, the Convention requires that national regulatory authorities be provided with adequate authority, competence, and financial and human resources to fulfil their assigned responsibilities[48]. The nuclear safety legislation, as adopted under the Euratom Community, has reiterated these requirements by the Directive 2009/71/Euratom[49]. Taking the prospective deployment of microreactors into consideration, the implementation of these requirements will demonstrate a considerable challenge for national regulatory authorities. They have been designed to oversee a relatively limited number of large reactors operated in the state territory. With the arrival of

advanced nuclear technologies, the number of installations that will need surveillance and assessment will increase rapidly. At the same time, the prospective deployment of microreactors will also increase the demands on the qualifications of the official staff of the regulatory authorities. Undeniably, this will also have an impact on the financing of the regulatory regime.

Prospective microreactors' decentralised character will also impact the management of the nuclear waste they produce[50]. With this respect, the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management stipulates that nuclear waste «*should, as far as is compatible with the safety of the management of such material, be disposed of in the State in which it was generated*»[51]. In the Euratom Community, the obligation of the state to provide a repository to dispose of nuclear waste produced within its territory has been reconfirmed by Directive 2011/70/Euratom[52]. The prospectively increasing number of microreactors may, however, trigger the interest of concerned states in another solution, which has been presumed both under the Joint Convention[53] and under the Euratom Community[54]. Those countries where a microreactor will represent the only source of nuclear waste may be interested in international (shared) repositories to avoid the necessity to establish their own repository. However, international repositories may also represent an option for the disposal of nuclear waste in transboundary agglomerations and industrial parks, where microreactors will be deployed[55].

3.3. Location

The prospective location of future microreactors represents another significant difference in comparison to the large reactors[56]. The location of large reactors has been due to safety concerns that have traditionally been planned at a considerable distance from large urban settlements. The distance between urban settlements and nuclear installations is being covered by emergency planning zones (EPZ), which have been designed to protect the population from the potentially disastrous impacts of a nuclear incident[57].

In strict contrast, the current endeavours with microreactors envisage placing them in the centres of the cities. For example, the Swedish data centre operator

Bahnhof plans to operate a microreactor in the northeastern part of central Stockholm, an area populated by approximately 9,500 inhabitants[58]. The fact that the microreactor will be constructed underground will protect it from seismic activity, other natural hazards and also from potential terroristic attacks[59]. Thus, one significant precondition for any deployment of the microreactors in these locations is establishing special emergency planning zones, which will be tailor-made to the risks potentially arising from these advanced nuclear technologies. The task of the national regulatory authority, together with the IAEA, will be this.

3.4. Production

The number of producers of large reactors is somewhat limited. In stark contrast, the number of potential suppliers of microreactors is constantly increasing[60]. Thus, in the future, a potential buyer of these advanced nuclear technologies will have much more choices among suppliers of technologies than the current buyers of large reactors. A smooth transfer of these technologies will be very much more manageable when a shared understanding of safety standards is found between the national regulatory authority of the supplier and the regulatory authority of the buyer[61]. Such mutual recognition of certifications would dramatically contribute to a smooth transfer of technologies. The platform for such mutual recognition can be provided either by bilateral agreements between the concerned national regulatory authorities or by multilateral action (see below).

One must remember that miniaturisation hasn't been exclusive to nuclear technologies. A very similar process is pending in the space technologies sector, where small satellites, including nanosatellites (also referred to as CubeSats or NanoSats)[62], are being developed and deployed on a large scale. To establish a transparent and predictable legal framework for launching these installations, brand-new space acts have been adopted in the last few years on the national level in Europe (for example, in Portugal – in 2019, Luxembourg – in 2020, and Cyprus – in 2023) and beyond (in the United Arab Emirates – in 2023, in Brazil – in 2024). Consequently, one may observe a very rapid legislative reaction to the newly emerging technology worldwide. In the European Union, a legislative

initiative is currently pending to design and adopt an EU Space Law that will provide for an EU-wide basic standard in the sphere of safety.
The field of space legislation is inspirative in two ways: firstly, one may expect that as soon as a critical number of microreactors arrive on the market, national legislators will also commence establishing their own rules to address risks arising from these technologies. Secondly, the already-adopted national space acts may provide inspirational solutions on how to tackle the issue of miniaturisation. For example, the Portuguese Space Decree-Law of 2019[63] provides that space activities shall be subject to a compulsory license, which is to be issued by the competent national authority. In this respect, the Space Decree-Law has introduced two specific types of licences, which will authorise launch and/or return operations, as well as command-and-control operations. A unitary license (*licença unitária*) may be granted, which applies to each type of space operation and is awarded to the respective operator[64]. Also, space activities may be authorised by a global license (*licença global*) that applies to several space operations of the same type and is granted to the respective operator[65]. Having said this, one must bear in mind that any feature similar to a global licence is very alien to the classical system of nuclear law. This is because large reactors require profound and distinctive licensing concerning their unique characteristics. However, with respect to microreactors, which will imply much lower risk and will be much more numerous, licencing several installations in one act could represent a viable solution in the future[66].

4. Towards a modern nuclear law

On 9 July 2024, US President Joe Biden signed the Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2024 (the ADVANCE Act of 2024). The main aim of the newly adopted legislation is to «*provide incentives for developing and deploying new nuclear technologies, such as reduced licensing fees and prize awards for deploying such technologies*»[67]. The ADVANCE Act of 2024 provides for a tailor-made framework for small modular reactors (advanced nuclear reactors in the wording of the Act). While it does not mention microreactors explicitly, they will fall under the scope of application of this newly adopted legislation[68]. The reaction of the ADVANCE Act of 2024 to the

emergence of advanced nuclear technologies is twofold: On one hand, a comprehensive set of provisions is focused on American Nuclear Leadership. Pursuant to these provisions, the Nuclear Regulatory Commission (the NRC) must coordinate certain international activities with respect to the advanced nuclear technologies within respective international organisations[69]. Also, the NRC has been empowered to establish the "International Nuclear Reactor Export and Innovation Branch", to carry out such international nuclear reactor export and innovation activities as the NRC determines to be appropriate and within its mission[70]. Thus, a good portion of the provisions of the newly adopted ADVANCE Act of 2024 focuses on the USA's international activities in the field of advanced nuclear technologies.

Secondly, the ADVANCE Act of 2024 also introduced several provisions entitled Developing and Deploying New Nuclear Technologies. In contrast to the provisions mentioned above, these provisions focus on supporting the deployment of advanced nuclear technologies in the USA by reducing specific fees and introducing prize awards. A special regime is being established to help those advanced nuclear technologies that will serve non-electric applications, such as hydrogen production, medical isotope production, water desalinisation, etc[71]. Also, the newly established legislation has introduced a special regime for the deployment of advanced nuclear technologies to the brownfields[72].

The ADVANCE Act of 2024 is the first legislative act worldwide to address the phenomenon of miniaturisation in nuclear technologies. At the same time, its provisions reflect the fact that advanced nuclear technologies, including microreactors, are currently in their infancy. Thus, instead of providing detailed rules on their licencing and operation, the ADVANCE Act of 2024 merely provides support for further development on a domestic and international level.

Despite the potential benefits the microreactors may bring, no similar legislation has been passed in Europe so far. One may expect that the gradual deployment of advanced nuclear technologies will also trigger legislators in Europe to provide transparent and competitive national rules in this field. Such legislative amendment has been recently adopted in Sweden[73]. However, the microreactors also represent a salient challenge for the Euratom Community itself[74]. While any rules in domestic legislation are missing, the Euratom Community represents a platform for setting basic safety and liability rules for these new types of nuclear

technologies. At the same time, the Euratom Community is also capable of establishing a framework for mutual recognition of certifications and, consequently, enabling easy circulation of technologies. In the same fashion as the field of space technologies, establishing common European rules will strengthen European autonomy also in the field of advanced nuclear technologies. At the same time, it will make Europe more competitive, transparent, and attractive to innovators.

Having said this, the authors of this article believe that future modern nuclear law must be capable of addressing all peculiarities arising from the miniaturisation of advanced nuclear technologies. Very similar to the field of space law, the law governing advanced nuclear technologies must also follow those basic principles, as recently recognised by the international community of States[75]. Any future legal framework must first respect the principle of nuclear safety[76]. Also, the permission principle[77] and the continuous control principle[78] must be applicable to advanced nuclear technologies. The same applies to the compensation principles, which call for adequate compensation in the event of a nuclear accident. However, all these principles must be considered in future legislation in the way peculiarities of technological miniaturisation will be reflected.

5. Conclusions

Data usage and global internet traffic have experienced exponential growth since the mid-2000s, and the trend is expected to continue and even accelerate due to the wide adoption of artificial intelligence. The total global energy demand for data centres now exceeds the consumption of most economies, and they emit around 2% to 4% of global greenhouse gas emissions. To meet this demand, data centre planners must consider not only the affordability aspects but also sustainability, supply security, and social impact. In this respect, nuclear microreactors have been recently discussed as a comprehensive, emission-free and renewable-led solution for powering the data centres. Several MoUs have been signed during the last few years, and they envisage the deployment of microreactors as a source of power for data centres in the forthcoming decade. Microreactors demonstrate several significant challenges that differentiate them

from large (conventional) reactors that have been in operation until now. Their miniature character implies a considerable decrease in risks arising. Also, they may serve as a tool for the decentralisation of power supply and can be located right in the very centre of urban settlements. Lastly, microreactors will be very easily transportable by land, sea, or air.

This article argued that the future deployment of microreactors does imply a considerable paradigm shift towards a modern nuclear law. This is very similar to the space sector, where space law has been needed to address the gradual deployment of small satellites; also, nuclear law is currently being triggered to establish new rules, reflecting this paradigm shift arising from miniaturisation. The ADVANCE Act of 2024, adopted very recently in the USA, represents only the very first legislative reaction worldwide to the phenomenon of miniaturisation in nuclear technologies. This article envisages that many others will come and urges the Euratom Community to take an active role in this process.

1. This paper was written under the umbrella of the project "*A fleet of small modular reactors on the horizon! Do we need a new nuclear law?*" (registration number 24-10062S), supported by the Czech Science Foundation.
2. See D. Rehman, P. Faria, L. Gomez, Z. Vale, *Future of energy management systems in smart cities: A systematic literature review,* in *Sustainable Cities and Society,* 96, 2023, article 104720.
3. See P. T. I. Lam, D. Lai, Ch. Leung, W. Yang, *Data centers as the backbone of smart cities: principal considerations for the study of facility costs and benefits*, in *Facilities,* 39, 2021, pp. 80-95.
4. See N. Ortar, A. R. E. Taylor, J. Velkova, P. Brodie, *Powering 'smart' futures: data centres and the energy politics of digitalisation,* in S. Abram, K. Waltorp, N. Ortar, S. Pink (eds), *Energy Futures*, De Gruyter, Berlin, 2023, pp. 125-168; F. Molnár, *Smart Solutions for Securing the Power Supply of Smart Cities,* in *Interdisciplinary Description of Complex Systems,* 21, 2023, pp. 161-167; T. Cioara, I. Anghel, I. Salomie, M. Antal et al., *Exploiting data centres energy flexibility in smart cities: Business scenarios*, in *Information Sciences,* 476, 2019, pp. 392-412; F. Niedermeyer, W. Duschl, T. Möller, H. de Meer, *Increasing Data Centre Renewable Power Share Via Intelligent Smart City Power Control,* in *e-Energy '15: Proceedings of the 2015 ACM Sixth International Conference on Future Energy Systems*, pp. 241-247 etc.
5. See D. Chernicoff, *As SMRs Stumble, Will Microreactors Find a Home In the Data Center Industry?,* https://www.datacenterfrontier.com/energy/article/33015713/as-smrs-stumble-will-micr

oreactors-find-a-home-in-the-data-center-industry [accessed on 17th December 2025].

6. See https://www.datacenterdynamics.com/en/news/bahnhof-wants-to-build-a-nuclear-power-station-for-its-new-stockholm-data-center/ [accessed on 17th December 2025].
7. See https://www.datacenterdynamics.com/en/news/nano-and-blockfusion-to-deploy-nuclear-microreactors-at-niagara-falls-data-center/ [accessed on 17th December 2025].
8. See https://www.theguardian.com/technology/2024/oct/15/google-buy-nuclear-power-ai-datacentres-kairos-power [accessed on 17th December 2025].
9. See https://www.neimagazine.com/news/nano-partners-with-digihost-on-nuclear-powered-ai-data-centre/?cf-view [accessed on 20th December 2024].
10. See S. Paul, M. Klimenka, F. Duarte, C. Crawford et al., *When Cities Go Nuclear: Exploring the Applications of Nuclear Batteries Toward Energy Transformation*, in *Urban Science,* 8, 2024, at pp. 226-246; A. Grishina, M. Chinnici, A. Kor, E. Rondeau et al., *Data Center for Smart Cities: Energy and Sustainability Issue,* in F. Pop, G. Neagu (eds), *Big Data Platforms and Applications. Case Studies, Methods, Techniques, and Performance Evaluation*, Springer Nature. Cham, 2021, at pp. 1-39.
11. See G. Black, D. Shropshire, K. Araújo, A. van Heek, *Prospects for Nuclear Microreactors: A Review of the Technology, Economics, and Regulatory Considerations,* in *Nuclear Technology,* 209, 2023, pp. 16-17.
12. For terminological clarification, see A. B. Frazier, R. O. Warrington, C. Friedrich et al., *The miniaturization technologies: past, present, and future,* in *IEEE Transactions on Industrial Electronics,* 42, 1995, pp. 423-430.
13. See J. N. Pelton, S. Madry, *Introduction to Small Satellites Revolution and Its Many Implications*, in J. N. Pelton, S. Madry (eds), *Handbook of Small Satellites Technology, Design, Manufacture, Applications, Economics and Regulation*. Springer Nature, Cham, 2020, pp. 1-33.
14. See A. Forganni, *Legal Considerations on Space Commercialisation,* in S. Lieberman, H. Athanasopoulos, T. Hoerber (eds), *The Commercialisation of Space Politics, Economics and Ethics*, Routledge, Cheltenham, 2023, pp. 211-227.
15. See L. Cesari, J. Handrlica, A. Sandulli, *Symposium on "Golden Age of European Space Regulation",* in *The Lawyer Quarterly,* 14, 2024, pp. 552-553.
16. See G. Mastroianni, *Il DDL Spazio italiano: le nuove governance, il dubbio sulla disciplina dei voli sub orbitali e l'allontanamento dal modello USA*, in Quaderni AISDUE - Rivista quadrimestrale, 2, 2024, pp. 1-25.
17. See L. Cesari, *Developing an EU Space Law: the process of harmonising national regulations*, McGill Institute of Air & Space Law, Montreal, 2024, available at https://www.mcgill.ca/iasl/article/developing-eu-space-law-process-harmonising-national-regulations [accessed on 17th December 2025].

18. See OECD/NEA, *Small Modular Reactor Dashboard.* 2nd edition, OECD, Paris, 2024, available at https://www.oecd-nea.org/jcms/pl_90816/the-nea-small-modular-reactor-dashboard-second-edition [accessed on 17th December 2025].
19. Argentina, Belgium, Canada, China, Czech Republic, France, Indonesia, Japan, Myanmar, Philippines, Poland, Romania, Russia, Rwanda, Saudi Arabia, South Korea, Sweden, Ukraine and the United States of America.
20. See J. P. Schlegel, P. K. Bhowmik, *Small modular reactors,* in J. Wang, S. Talabi, S. Bilbao y Leon (eds), *Nuclear Power Reactor Designs*, Academic Press, Cambridge, 2023, pp. 283-308.
21. Cement, chemicals and petrochemicals, and steel industries. These industries are responsible for nearly 60 per cent of total industrial energy consumption and contribute approximately 70 per cent of industrial CO2 emissions.
22. See C. Stenberg, *Energy transitions and the future of nuclear energy: A case for small modular reactors,* in *Washington Journal of Environmental Law & Policy,* 57, 2020, pp. 57-73.
23. See A. Vaya Soler, *The future of nuclear energy and small modular reactors*, in T. Letcher (ed), *Living with Climate Change*, Elsevier, Amsterdam, 2023, pp. 465-512.
24. See J. Vujić, R. Bergmann, R. Škoda, M. Miletić, *Small modular reactors: Simpler, safer, cheaper?,* in *Energy,* 45, 2012, pp. 288-295.
25. See https://www.iaea.org/newscenter/news/what-are-small-modular-reactors-smrs [accessed on 17th December 2025].
26. See R. Testoni, A. Bersano, S. Segantin, *Review of nuclear microreactors,* in *Progress in Nuclear Energy,* 138, 2021, article 103822.
27. See IAEA (ed), *Small Modular Reactors. Advances in SMR Developments 2024*, IAEA, Vienna, 2024, p. 13.
28. See https://www.energy.gov/ne/articles/what-nuclear-microreactor [accessed on 20th December 2024].
29. See IAEA (ed), *Small Modular Reactors. Advances in SMR Developments 2024*, IAEA, Vienna, 2024, pp. 14-15. For a significantly updated overview of ongoing projects, see T. Lane, S. T. Revankar, *Advances in technology, design and deployment of microreactors- a review*, in *Progress in Nuclear Energy,* 178, 2025, article 105520.
30. See https://westinghousenuclear.com/energy-systems/evinci-microreactor/ [accessed on 17th December 2025].
31. See https://www.datacenterfrontier.com/energy/article/55232808/westinghouse-evinci-microreactor-could-yield-5-mw-of-nuclear-power-every-8-years-for-ai-data-centers [accessed on 17th December 2025].
32. See https://nanonuclearenergy.com/microreactors/ [accessed on 17th December 2025].
33. A pioneering project of a university microreactor is currently being realised at the Lappeenranta University of Technology in southeastern Finland. In 2022, this University

signed a Memorandum of Understanding with the Seattle-based *Ultra Safe Nuclear Corporation,* aiming to deploy a microreactor as a research and test reactor in the city of Lappeenranta, which is the regional capital of South Karelia.

34. See https://www.theguardian.com/technology/2024/oct/15/google-buy-nuclear-power-ai-datacentres-kairos-power [accessed on 17th December 2025].
35. See R. Sam, T. Sainati, B. Hanson, R. Kay, *Licensing small modular reactors: A state-of-the-art review of the challenges and barriers,* in *Progress in Nuclear Energy,* 164, 2023, article 104859, p. 2.
36. See K. Sexton Nick, *The future of nuclear energy and the role of nuclear law*, in *Nuclear Law Bulletin,* 2022, pp. 9-11.
37. See Z. Zhang, C. Wang, K. Guo, S. Qui et al., *Microreactors,* in J. Wang, S. Talabi, S. Bilbao y Leon (eds), *Nuclear Power Reactor Designs*, Academic Press, Cambridge, 2023, pp. 309-347.
38. See B. Newsad, *Micro Nuclear Reactors Can Help Solve the Climate Crisis,* in *Environmental, Natural Resources & Energy Law Blog,* Lewis & Clark Law School, available at https://www.lclark.edu/live/blogs/227-micro-nuclear-reactors-can-help-solve-the-climate [accessed on 17th December 2025].
39. See H. Cook, *The Law of Nuclear Energy*, 3rd edition, Sweet & Maxwell, London, 2022, pp. 410-412.
40. Convention on Nuclear Safety, art. 7.2.ii.
41. For further details, see A. Van Kalleveen, *Applicability of the international nuclear legal framework to small modular reactors (SMRs). Preliminary Study*, European Commission – Joint Research Centre, Brussels, 2022, p. 4.
42. Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations**,** OJ L 172, 2.7.2009, pp. 18–22, art. 4.1.b.
43. See R. Sam, T. Sainati, B. Hanson, R. Kay, *Licensing small modular reactors: A state-of-the-art review of the challenges and barriers,* in *Progress in Nuclear Energy,* pp. 2-6; T. Sainati, G. Locatelli, N. Brookes, *Small Modular Reactors: Licensing constraints and the way forward,* in *Energy,* 82, 2015, pp. 1092-1095.
44. See J. Handrlica, M. Novotná, *The feast of insignificance of small modular reactors in international nuclear law,* in *Czech Yearbook of Public & Private International Law,* 12, 2021, pp. 327-328.
45. For more details on the liability issues arising with respect to the small modular reactors, see V. J. H. Roland, *Applicability of the existing nuclear liability conventions to different types of small modular reactors currently under development,* in *Nuclear Law Bulletin,* 110, 2023, pp. 7-36.
46. See J. R. Lovering, *A Techno-Economic Evaluation of Microreactors for Off-Grid and Microgrid Applications,* in *Sustainable Cities and Society,* 95, 2023, article 104620.

47. Convention on Nuclear Safety, art. 7.2.iii.
48. *Ibid*., art. 8.1.
49. Directive 2009/71/Euratom, art. 4 and 5.
50. See B. Zohuri, *Nuclear Micro Reactors*, Springer Nature, Cham, 2020, pp. 110-115.
51. Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, Preamble at (xi).
52. Council Directive 2011/70/Euratom of 19 July 2011 establishing a Community framework for the responsible and safe management of spent fuel and radioactive waste, art. 4.4.
53. Joint Convention, Preamble at (xi).
54. Council Directive 2011/70/Euratom, art. 4.4.
55. See N. Prieto Serrano et al., *SMR and AMR Radioactive Waste: A Comparative Legal Analysis*, paper presented at the 25th Nuclear Inter Jura Congress in Warsaw in November 2024 and available here: https://dise.org.pl/papers/S10_Nuria_Prieto-Serrano_Waste_from_SMR_Inter_Jura_Warsaw_2024_with_Annex_USA.pdf [accessed on 17th December 2025].
56. See A. Larson, *Is a Nuclear Reactor Headed to the Heart of Your City?*, available at https://www.powermag.com/is-a-nuclear-reactor-headed-to-the-heart-of-your-city/ [accessed on 17th December 2025].
57. The emergency planning zone (EPZ) is defined by the IAEA as «*the precautionary action zone (PAZ) and the urgent protective action planning zone (UPZ)*» See IAEA (ed), *Preparedness and Response for a Nuclear or Radiological Emergency*, in *IAEA Safety Standards Series No. GSR. Part 7*, IAEA, Vienna, 2015, p. 82. The precautionary action zone (PAZ) and the urgent protective action planning zone (UPZ) are defined in the same publication on p. 91 (PAZ) and p. 96 (UPZ).
58. See https://sv.wikipedia.org/wiki/Hjorthagen [accessed on 17th December 2025].
59. See D. Dalton, *Underground Plants 'Could Be Built In City Centres',* https://www.nucnet.org/news/underground-plants-could-be-built-in-city-centres-11-3-2024.
60. See D. Shropshire, G. Black, K. Araújo, *Global Market Analysis of Microreactors*, Idaho National Laboratory, Idaho Falls, 2021, pp. 61-86.
61. For a much more detailed study on this problem, see T. P. Kuipers, *Developing nuclear security related legislative guarantees in licensing mobile Small Modular Reactors*, Master Thesis, Department of Business and Management at the University of Applied Sciences Brandenburg, 2020.
62. Nanosatellites are small satellites that typically weigh less than 10 kilograms and measure from 10 centimetres to 10 x 10 x 11.35 centimetres in size. They provide a range of applications, including communications, Earth observation, remote sensing, and scientific research.
63. Decreto-Lei n.º 16/2019, de 22 de janeiro.
64. *Ibid*., art. 6.1.a.

65. *Ibid.*, art. 6.1.b.
66. See F. Ekinci, M. S. Guzel, K. Acici, T. Asuroglu, *The Future of Microreactors. Technological Advantages, Economic Challenges, and Innovative Licensing Solutions*, in *Applied Sciences,* 14, 2024, article 6673.
67. See https://www.congress.gov/bill/118th-congress/senate-bill/1111 [accessed on 17th December 2025].
68. See ADVANCE Act of 2024, Sec. 2.4.
69. *Ibid.* Sec. 101.
70. *Ibid.* Sec. 101.b.
71. *Ibid.* Sec. 203.c.
72. *Ibid.* Sec. 206.
73. On 1 January 2024, new rules for when nuclear power plant reactors may be built took effect in Sweden, allowing new reactors to be established in areas where nuclear power plants have previously not been located. This will virtually enable the construction of microreactors in the future. See https://www.loc.gov/item/global-legal-monitor/2024-01-29/sweden-new-rules-for-nuclear-power-plant-reactors-take-effect/ [accessed on 17th December 2025].
74. See P. Gorzkowski, *Legal barriers to the deployment of SMR and ANT reactors in the European Union. Is the Euratom Treaty sufficient?*, paper presented at the 25th Nuclear Inter Jura Congress in Warsaw in November 2024 and available here: https://dise.org.pl/papers/S13_Przemyslaw-Gorzkowski.pdf [accessed on 17th December 2025].
75. See J. Handrlica, *Nuclear law revisited as an academic discipline,* in *The Journal of World Energy Law & Business*, 12, 2019, pp. 52–68.
76. See C. Stoiber, A. Baer, N. Pelzer, W. Tonhauser, *Handbook on Nuclear Law*, IAEA, Vienna, 2003, p. 5.
77. *Ibid*. p. 7.
78. *Ibid*. p. 8.

Energy communities for smart cities: a challenge for EU administrative law in light of the Italian perspective

Alessia Monica, Leonardo Scuto

DOI: 10.13130/2723-9195/2025-1-86

Il presente contributo assume la smart city come "paradigma" delle politiche ambientali ed energetiche dell'UE, nel solco del Green Deal. Pertanto, le Comunità energetiche nelle smart city dovrebbero essere un motore per la transizione energetica, nonché un modo per affrontare l'emergenza climatica. In questo senso, descrivendo le Comunità Energetiche Rinnovabili (CER) sviluppate in Italia, si delinea il ruolo del "cittadino" come parte di una comunità intelligente che deve essere promossa e implementata sia dall'UE che dagli Stati membri. In questo percorso, il principio di leale cooperazione, che consente di affrontare le questioni amministrative transfrontaliere certamente presenti nelle CER, rappresenta un principio flessibile (con pro e contro) per assicurare gli interessi delle generazioni future, senza trascurare gli obiettivi di sostenibilità.

The paper assumes a commitment to smart cities as a "paradigm" in EU environmental and energy policies, having the Green Deal in the background. Energy Communities in smart cities are supposed to be a driver for the green energy transition, as a way to deal with the climate emergency. Renewable Energy Communities (REC) as developed in Italy demonstrate the role of the "citizen" as part of a smart community – which can be promoted and implemented by both EU and Member States. The principle of sincere cooperation is a flexible principle that can assure the interests of future generations, while not neglecting sustainability goals in order to address cross-border administrative issues present in REC.

framework: a driver for energy transition, as well as a way to deal with the climate emergency.- 2.1. Renewable Energy Communities in Italian legislation.- 2.2. The Energy Communities: scope of activities and members.- 3. EU and Member States administrative cooperation in decision-making processes related to Renewable Energy Communities.- 4. The EU administration as result-oriented towards the rights of future generations.

1. Introduction: the Smart City as a "paradigm" in the EU environmental and energy policies

To date, there is no agreed definition of smart cities, even in legal scholarship[2], whereas there is a definition of Renewable Energy Communities (hereinafter, "REC(s)")[3]. This deficit is explained by the presence of diverse extra-legal fields in the very nature of smart cities[4], leading to difficulties of coordination as well as a complex intertwining of multilevel competencies that, precisely, have consequences on the definitional level. Obviously, public law is called upon to grasp the legal problems of every area where ICT technologies are used to implement public policies, as in the specific case of the urban context concerning smart cities. Moreover, in a field where the urban planning and regulation challenges are matched by another area of intervention of the public decision maker- such as the energy sector- characterized, itself, for the complexity of its assets and of a multilevel governance. Therefore, the present article, examines smart cities from the perspective of key sectors such as energy, linking it with the energy transition and efficiency, as well as the climate protection which need to be taken into account in today's debate.

From their side, energy communities, referring to forms of organizing activities underpinned on «*renewable energy, localness (...) participation of various actors*» in comparison to conventional large-scale industries[5], indeed, are set in a supranational context in which ICT are pre-eminent for their proper functioning from the citizens' point of view. It is therefore worth briefly describing the starting context: smart cities as a paradigm within EU environmental policies (and not only environmental law) whose implementation is a duty of the Member States (§1).

The examples of implementation of energy communities (REC) in Italy (§2) will offer food for thought on which a broader reflection might be launched. Consequently, REC are complex systems in which different (European and national) policies and competences are intertwined and, as a result, the leading idea of this article is that administrative cooperation plays a crucial role for the effective success of these communities (§3). Besides, looking at EU and MS administrative activity as result-oriented[6], effective decisions must be taken as to cope with the protection of future generations first and foremost (§4).

Against this background, smart cities can be imagined as models of declination, hence paradigms[7], of experiences related to REC where the technological dimension, basically standing on data[8], is at the heart of its evolution. Smart cities are therefore a hub of digital transition[9] but also a place of institutional experimentation closely linked to the control of urbanisation where it is recognised that the centrality of planning is also a tool for patrol the new dangers of society[10] with regard to public interest[11]. Therefore, in smart cities the community is placed at the centre of both the administrative function and the organisational function[12] where «*the collective dimension appears to be essential and prevailing, whereby the limitation of individual freedom is regarded as a "smart" measure to adopt when necessary*»[13].

As already said, legal issues are far-reaching, because of the risk society demanding to make the administration reflexive and ready for new forms of cooperation with the private sector[14] and to be geared towards exercising authorisation functions on an adaptive approach (which is allowed by data exploitation).

Policies promoting smart cities are then closely interrelated to environmental policies and, in the present article, are also to be considered as part of energy policies. Or rather, it will be highlighted the smartness[15] set in REC as part of urban development[16]: «*smart and green characteristics of communities are linked as regards smart buildings and more widely, smart environment*»[17]. For both the environment and energy, the Union exercises a competence shared with the Member States (art. 4 TFEU); while for all matters concerning technological developments, the legal basis for the adoption of an EU act is linked to the policy area in which the specific action fits. Accordingly, the material scope of application of EU law concerning environment, energy and ICT are determined by the principle of conferral. Albeit the specific legal basis for the environment

policy are particularly «*well drafted*»[18], together with energy, they are both field of policies bordering the internal market as well. Referring directly to the Lisbon Treaty it is self-evident how the establishment of the internal market (art. 3 TEU) is strictly linked with other goals related with public interest such as the environment (and sustainable development)[19] and social progress, therefore administrative function carried out in environmental policies at the EU level based on a shared competence are increasingly implemented through intertwined models of administration, leading to two considerations. The first concerns the structure of competences (and the use of implicit powers) where the objectives connected to environmental regulation do not strictly cover environmental policies, but are part of the regulation of social activities; the latter are rather coordinated starting from the EU level by leaving the Member States wide discretionary powers regarding the content of the implementation measures. This is precisely the case of the energy sector, where the security and affordability of supply are not only social issues embedded in the broader concept of sustainability[20] but they are closely linked to the opening of the market to competition and its promotion, although the opposite is also true. For example, competition leads to a more conscious choice by the consumer[21], especially the small consumer who, however, is in the so-called «*evolved supply chain*» expression of the ecological transition, is no longer only passive, but is also encouraged to widespread production. Energy supply in the free market (of energy as a good[22]) is, however, again a global problem closely linked to the fundamental rights of environment protection, as well as the goal of climate neutrality by 2050 established in the Green Deal[23].

So, if the smart city is *smart* and *efficient* through the use of technology, all the more reason for REC to take into account the environmental and sustainability dimensions, as already hoped by United Nations Economic Commission for Europe (UNECE) defining «*Smart Sustainable Cities*».[24] This pathway has also inspired EU policies on smart cities, hopefully gazing at future generation[25], with respect to economic growth, social and environment dimensions merged all together[26].

2. Energy Communities in the EU legal framework: a driver for energy transition, as well as a way to deal with the climate emergency

In light of the strategy introduced by the EU in the field of energy sector[27], citizen-consumers (i.e. *prosumers*) are called to play an active role, participating – within their communities – in the transition to climate neutrality, no longer as (passive) consumers of energy, but as (active) producers of it.

The EU's aim is to support the evolution of the role of the energy consumer, making them active energy-producing citizens, or, in other words, *prosumers*[28].

This means, as will be better discussed below, that the energy *prosumer* is the person who owns his own energy production plant, of which he uses – for his own needs – only a portion of the capacity produced; the residual can be fed into the grid, exchanged with other users or even accumulated in storage systems and, subsequently, returned to the consumption units at the most appropriate time[29].

In line with the EU's energy strategies, one of the most important tools ensuring the active participation of citizens, in the dual role of passive and active users, according to the terms outlined above, is manly represented by the Renewable Energy Communities (hereinafter, the "REC(s)").

These, in fact, can be defined as «*an organisational model endowed with legal subjectivity that allows participants to carry out, in an institutionalised form, a whole series of activities in the energy sector ranging from the generation, distribution, sale, conservation, purchase of energy, to the implementation of energy efficiency services, in order to produce environmental, economic and social benefits*»[30].

In this sense, a first and important legal recognition was introduced, for the first time in EU law, precisely by the Directive EU/2018/2001 (also known as the Renewable Energy Directive (RED II)[31], as transposed in Italy by Legislative Decree No. 199 of 8 November 2021[32] and, secondly, by Directive EU/2019/944 on "*common rules for the internal market for electricity (...)*"[33], subsequently transposed by Legislative Decree No. 210 of 8 November 2021[34], which defined, each to the extent of its competence, the concepts of Renewable Energy Community and Citizen Energy Communities (hereinafter, "CEC(s)")[35].

An analysis of the definitions offered, in the first instance, by EU law shows that both of the above-mentioned configurations (i) are legal entities separate from their members (unlike the model called "collective self-consumption" (*autoconsumo collettivo*)[36]), (ii) are organised on a voluntary basis, (iii) pursue mutualistic purposes (i.e. provide environmental, economic or social benefits to their members and the territory where they are based), and (iv) are required to carry out activities involving energy products.

To the same extent, the same configurations nevertheless present some differences, which can be identified (i) in the different requirements of the corporate structure (only natural persons, Small and Medium Enterprise (hereinafter, "SME(s)") or local authorities can join a REC, whereas no subjective qualification is required to take part in an CEC[37]), (ii) in the ownership of the energy production plants (for RECs, the plants must belong to or be developed, at least according to EU law, by the REC itself; whereas in the case of CECs, they may also use the installations of others), (iii) in the proximity or physical proximity to the plants[38], (iv) in autonomy (the REC must in fact correspond to a legal entity "autonomous" with respect to its individual members[39]), (v) in the different types of energy activities that they may carry out (whereas CEC must carry out activities concerning electricity produced from any source, REC must carry out activities related exclusively to energy products based on renewable non-fossil sources).

Despite these differences, both configurations represent a form of «*democratisation of the energy system*»[40], realised through two important factors: co-ownership of the means of production of renewable energy, and co-management of the means of distribution that allows users to be – at the same time – producers, consumers and managers of renewable energy.

Therefore, RECs, from the EU legislator point of view, represent «*an effective and cost-efficient way to meet citizens' needs and expectations regarding energy sources, services and local participation*, as they represent. *Community energy offers an inclusive option for all consumers to have a direct stake in producing, consuming or sharing energy*», as they represent «*an inclusive option for all consumers to have a direct stake in producing, consuming or sharing energy*»[41].

Finally, it should be noted that it would seem possible to detect a *favour* on the part of the EU legislator[42] – as highlighted by the relevant literature[43] – towards

this instrument, providing, with reference instead to the CECs, that Member States are required to establish «*regulatory framework for citizen energy communities (...)*» (see art. 16 of Directive EU/2019/944); while, with regard to RECs, they must provide «*enabling framework to promote and facilitate the development of renewable energy communities*» which must, among other things, also guarantee the presence of a whole series of instruments aimed at supporting and facilitating the development of the RECs themselves (see art. 22(4) of Directive 2018/2001/UE).

Hence, an REC is an organisation of citizens, businesses, local authorities and others who freely and democratically take part in the production, management and exchange of renewable energy, thus enabling the latter to become protagonists in the energy system.

According to these considerations, therefore, it is possible to state that RECs are true vectors of the energy transition, being considered, first and foremost by the European legislator, an essential tool for the development of the production and use of renewable energy sources.

Lastly, such configurations represent the milestone of the energy transition, giving flexibility to the energy system through the decentralisation of production, as better explained *infra*.

2.1. Renewable Energy Communities in Italian legislation

The RED II Directive was definitively transposed in Italy through, *inter alia,* Legislative Decree No. 199/2021, which – also on the basis of what emerged from the experiments carried out during the so-called "transitional period"[44] – innovated the main characteristics of the RECs, as well as instructing the Italian Regulatory Authority for Energy Networks and the Environment (*Autorità di Regolazione per Energia Reti e Ambiente*, "ARERA"), the Ministry of Environment and Energy Safety ("MEES") and the Energy Services Operator (Gestore dei Servizi Energetici, "GSE") to update, respectively, their regulations, the incentive regime, and the operating rules[45].

The main innovations introduced by the aforementioned legislative decree essentially consist of (i) the extension of participation – in addition to natural persons, SMEs and territorial entities – to research and training, religious, third

sector and environmental protection entities, (ii) the possibility of receiving an incentive on shared energy through plants with a capacity of up to 1 MW[46], (iii) the connection of plants and utilities under the same primary cabin.
The resulting enlargement of the geographical perimeter, therefore, has made it possible to build plants capable of meeting the energy needs of much larger communities than those initially envisaged by the so-called "transitional regime".
Another important innovation, as far as the accounting of virtually shared energy is concerned, is the fact that – thanks to the new regime – only the production of renewable energy of plants that are in the availability and under the control of RECs, which came into operation after the date of entry into force of Legislative Decree No. 199/2021, are taken into account[47].
Finally, it is interesting to note that Article 14 of the same legislative decree defined specific criteria for coordination between the measures introduced by the National Recovery and Resilience Plan (hereinafter, the "NRRP")[48] and sectoral incentive instruments[49].

2.2. The Energy Communities: scope of activities and members

Before going further into the analysis concerning the scope of activities and the actors that may participate in a REC, it must be considered that, under the TIAD, the more general configuration of the so-called "diffuse self-consumption" (*autoconsumo diffuso*) is expressed in several micro-categories of configurations with different characteristics and connotations, and in particular:

1. individual self-consumer of renewable energy 'at a distance' (*autoconsumatore individuale di energia rinnovabili "a distanza"*) using the distribution network (hereafter, as considered by the GSE Operating Rules, "Self-consumer at a distance");
2. individual 'remote' renewable energy self-consumer with direct line (*autoconsumatore individuale di energia rinnovabile "a distanza" con linea diretta*);
3. group of self-consumers of renewable energy acting collectively (*gruppo di autoconsumatori di energia rinnovabile che agiscono collettivamente*)

(hereafter, as considered by the GSE Operating Rules, "Self-Consumption Group");
4. group of active customers acting collectively (*gruppo di clienti attivi che agiscono collettivamente*);
5. active 'remote' customer using the distribution network (*cliente attivo "a distanza" che utilizza la rete di distribuzione*);
6. Citizens Energy Community (i.e., the CEC); and
7. Renewable Energy Community (i.e., REC), the subject of this discussion.

For a full analysis of the above-mentioned typologies (see, in particular, (a), (b), (c), (d), (e), (f)), please refer to the relevant literature[50], choosing to focus a more complete analysis on the subject of this discussion, i.e., RECs.

This having been said and considered, with reference to the activities that a REC can carry out, the applicable regulations emphasise, first and foremost, the role that these configurations take on in the electricity market, providing, in particular, that they can produce, store and share the electricity produced by the plants at the REC's disposal, or, even more importantly, sell the surplus energy produced to the grid, also through sale and purchase agreements.

Therefore, RECs will be able to take on two important roles, namely (i) limiting themselves to acting as an aggregator of the various *prosumers* in order to maximise the profitability of the plants they hold (this thanks to access to the incentive schemes provided for by MEES Decree no. 414/2023[51]), or (ii) take an active role within the energy market, qualifying itself as a producer in relation to the energy generated by the plants it owns (or of which it has availability), through (a) the sale of energy on the market or (b) by entering into special energy sales contracts (i.e., power purchase agreements[52]) with market counterparties.

In addition, the priority role of the REC certainly remains that of valorising virtual self-consumption, since*, by law,* it plays the role of 'referent' and is therefore the party appointed to sign the agreements with the GSE, as well as to receive the benefits deriving from the incentive mechanisms and valorisation of virtual self-consumption.

However, Legislative Decree No. 199/2021 identifies additional services that Energy Communities will be able to perform while respecting – keep this in mind – the primary objective of providing environmental, economic and social

benefits to their members and the community (certainly not that of making financial profits).
In this sense, the REC will be able to provide, among others, energy efficiency services and electric vehicle charging services.
Finally, with regard to the subjects, as partially already mentioned, Article 37(1)(b) of the aforementioned Legislative Decree defines the RECs as a «*subject of autonomous law*»[53], and then provides a list of members that may exercise the power of control, namely (i) natural persons, (ii) SMEs (provided that participation in the ERCs does not constitute the prevailing commercial or industrial activity), (iii) territorial entities and local authorities (including municipal administrations), research and training entities, religious entities *et similia*.
In this respect, an important innovation was introduced by Decree-Law No. 13[54] of 24 February 2023, which added «*associations with legal personality under private law*»[55], i.e., recognised associations, to the previous list.
In light of the above, it is possible to identify essentially four fundamental roles that the actors involved in the operation of an REC may play, namely:

1. the consumer member of the REC;
2. the consumer-producer member of the REC (i.e. the *prosumer*);
3. the external producer who is not a member of the REC; and
4. an external entity that makes facilities or land available for the benefit of the non-member REC.

The aforementioned Decree has also specified that the Energy Community must consist of a legal entity of a collective nature subject to specific requirements concerning its establishment and operating conditions[56].
Pursuant to the "autonomy requirement", the REC must have a democratic structure, as recalled in Recital 71 of RED II, according to which «*renewable energy communities should be capable of remaining autonomous from individual members and other traditional market actors that participate in the community as members or shareholders, or who cooperate through other means such as investment*».
Finally, as far as it is of specific interest, a central element – as identified in Recital

70 of RED II – is the active involvement of citizens and local authorities in the definition of the *governance* policies of the REC itself[57].

3. EU and Member States administrative cooperation in decision-making processes related to Renewable Energy Communities

As formerly implied, regulating REC already from the EU level entails surfing different policy areas sweeping over also administrative activities because of the effort to «*recognise certain categories of citizen energy initiatives at the Union level as 'citizen energy communities'*»[58] affecting, first of all, the right of participation in a procedure as a component of the *governance* of the energy market as a whole. As already clarified, REC are complex systems set in a multilevel legal context where "*twin transition*" are intertwined together. In this way the principle of sincere cooperation is a mainstay, both for EU and both for Member States, to «*assist each other in carrying out tasks which flow from the Treaties*»(art. 4 TEU)[59] and facilitate the action of administrations[60] «*when dealing with cross-border issues*»[61] widening and deepening over the time as to reduce the national - based regulation of economic activities and fostering the internal market development[62]. But actually, cooperation cannot be slightly taken for granted, specifically with the *Green Deal* on the background[63]. There are several reasons for this, as to underpin the role of the Commission in cross-border situations, or to consider national implementation measures such as incentives.

To begin with, it is crucial ensuring that actions implemented by the MS by national measures in REC implementation are in full compliance with the EU law as to reach the full achievement of the goals of EU energy policies. But for climate neutrality, as the main goal of the Green Deal, it encompasses different measures achieving the decarbonisation and, on this path, energy is a strategic sector. As already clarified, REC are policy tools where the management and the regulation of the production are radically changed betting on renewable and clean energy sources and promoting new ways of distributions[64].

Against this backdrop public authorities are called upon to foster this new way of production, monitoring its functioning. Indeed, assuring "energy needs" through public service may constitute the subject of a social right affecting also public

interest[65] at the local context carrying out services of general economic interest, but with positive benefits on a large scale for the community. Thus, administrative cooperation is surely a duty but it might also be seen as a resource «*for the proper functioning of the Union*»[66]. For example, the Directive 2018/2001/EU on renewable energy specifically pushes «*cross-border participation*» as the natural corollary to the development of the Union renewable energy policy, fostering convergence and cooperation[67] to contribute to the Union's binding target. In this way, administrative cooperation is supposed to lead a complex legal scenario where also energy policy is to be integrated «*in environmental protection across EU policies and activities is also mandated by Article 11 TFEU*» [68] requiring, itself, cooperation between Member States and the EU, and between EU institutions, bodies and organisms. So, how the EU and Member States effectively meet its renewable energy targets? The Directive of 2019, for example, aims that the creation of a market framework that rewards flexibility and innovation would also be a the key factor enabling the uptake of renewable energy[69].

Again, the *Green Deal* aspire to develop a fully integrated, interconnected and digitalised EU energy market so that the Commission is the steering institution which is expected to enforce, implement and monitor the *Fit for 55 Strategy*. This package is going to cover a wide range of policy areas, including energy efficiency, renewables, land use, energy taxation, effort sharing and emissions trading. Concretely, among many others duties, it is the EU Commission which must foster REC development among MS. Therefore, the Commission's role of co-ordination, of encouraging good practices, and the role of energy regulators, starting with the EU regulator ACER, coordinating legislative action, to support a network that promote EU energy standards and technologies at global level. Hence, the principle of sincere cooperation can also represent "*a fallback provision on which the Commission can rely to underpin its supervisory functions*"[70] and implies mutual duties, as recently recalled by the CJEU in a case related to environmental protection, *Union de industries del la protection des plantes* C- 514/19[71]for EU institutions and bodies, as well as for Member States.

As has been well pointed out, REC are instruments for governing the energy and urban market, at the same way in which technical innovation can be a driving force for boosting their growth and efficient operation, assuring environmental

protection among EU and Members; meanwhile they are assumed as a "paradigm of sustainability" serving as the foundation for self-consumption arrangement[72]. Above all, REC pushes on the responsibility of the citizen as the person who, among other duties, is also entrusted with the various objectives of the energy transition. In particular, the energy efficiency undertaken through REC arises two main considerations. Firstly, it deals with the implementation by Member States of main targets of the *Green Deal* because of the lack of specific legislative acts providing binding measures and objectives as to comply with the ambitious goal of climate neutrality relying also on solidarity principle. The issue of implementation to be carried out by Member States is itself intertwined with administrative cooperation because of the composite-decision making procedures characterizing policy field of shared competence and requiring the active participation of both level, EU and MS, to be set. For example, energy community is often implemented through positive incentive schemes[73], such as in Italy, which are based on the freedom of choice of the individual, who can receive financial subsidies for carrying out a certain action[74]. As mentioned, the Decree 414/2023 merges 2 different types of incentives which can be also cumulated. Generally, the economic incentive is the benefit for having contributed to the pursuit of the public interest. Although, this aspect mainly concerns economic law and theories of regulation, it is not beyond the scope of administrative law considerations. Indeed, albeit the choice of this instrument is a specific expression of the procedural autonomy of the Member States, it can potentially lead to significant disparities in national energy markets with cross-border effects, which clearly also have an impact on the achievement of policy objectives in the energy sector at EU level. As explicated in the Directive 2019/944 Directive the energy market has to be «*Competitive, consumer-centred, flexible and non-discriminatory*»[75]. Inevitably, this regulatory provision, although not characterized by direct effect, should bind the Member States in the sense of not implementing actions that might disadvantage also cross-border situations. In this way also cross-border cooperation is crucial[76]; to make cross-border cooperation truly effective, under current legislation, principle of EU administrative law are to be relied upon. Even more, relying on principle of sincere cooperation may steer different administrations towards the right direction because it has to be applied also in internal situation[77] and it can

represent a support also to assure the full expression of the principle of good administration which has been recognised as a fundamental rights of EU citizens by art. 41 CDFEU[78], so, it is surely applied in cross-border situation. In a nutshell, the principle of sincere cooperation it's «*a connection between administrative power*»[79] and it rather refers to procedural rights such as the duty to provide information about the implementation of the Directive which conforming the conduct of the administration (for specific aspects) cannot be formalised according to pre-established rules[80], but they allow to reach the expected results so assuring an effective administrative action[81]. This is the case of "binding overall Union target for 2030" set in the Directive 2018/2001 as part of their integrated national energy and climate plans in accordance with Regulation 2018/1999/EU[82]. In other words, effectiveness[83] thus refers to the proportionality of the administrative choice, in relation to a fully europeanised situation. Moving back to the Italian legal framework, the incentives provided for REC are the specific tool the national administration has introduced as to comply with the NRRP), M2C2 – "*Renewable Energy, Hydrogen, Grid and Sustainable Mobility*".

The second critical point to be considered, instead, stems from the nature of the energy community. Thus, it is a model whose strength is likely based on the autonomy and responsibility of the community of reference. Again, it is a model of self-government that places the citizen at the centre of administrative action, starting from a bottom-up approach[84] that cannot, however, be separated from being part of a multi-level regulatory context where the transnational dimension cannot be underestimated.

Actually, according to the dual role played by the *prosumer* as "consumer and producers", or also as "regulator and addressee" of the regulation activity, two main issues are not to be undertaken for the implementation of the EU law.

First of all, the sincere cooperation must rely on the sharing of information[85] with the REC and among them not only at the national level. Secondly, the sharing activities implies the creation of data repository and the fulfilment of personal data process requirements. Besides invest on data allows for improved administrative activities, both in terms of action and relations. Actually, it can be claimed that REC are a meaningful expression of the *twin transition*, representing not only a driver for the energy transition but are also part of a smart

and sustainable city rooted on digital transition[86]. For example, efficient electricity grid is already smart in itself and to improve its smartness it must also rely on data and digitalisation to be resilient[87].

And on top of all of that, effective judicial protection of administered citizens is not only a concern with the system of administrative justice in the EU and integration between legal systems of MS, but rather an issue related to a new way of managing administrative power (shared with private actors in the REC), because a shortcoming of a strengthen cooperation is the "negative effects" on citizens protection against unlawful administrative decision[88]. Therefore, it is also a matter of accountability and democratic control Indeed, it is the case of a decision taken after a negotiation with private parties or when decision are also the example of a practice of co-regulation applying standard not previously defined in a binding act. Another aspect follows: of course it is the authority which has adopted the binding act which could be taken into a Court; but in a multilevel governance, the national authority or the EU Commission may challenge a decision (and its effects), may adopt safeguard measures (for example according more protection to "vulnerable consumers"[89]), may exercise powers of control or of withdrawal[90], with a substantive undermining of the cooperation activities carried out with private parties with an impact on their legitimate expectations. As well, private parties can act some administrative powers too[91].

Finally, the underlying challenge is to ensure that all citizens' interests are met as direct parties of the decisional process and pillars of a REC. The latter is also a component of the development of a smart city really aimed at producing social value[92], or directly providing services that improve energy efficiency. For example, Italian local authority must activate an energy management contract with the community[93], likely aspiring to become examples of best practice also from the administrative perspective as to be reproduced in other contexts.

4. The EU administration as result-oriented towards the rights of future generations

To conclude some remarks can be drafted pursuant to the principle of sincere cooperation: it is a flexible principle, maybe underestimated[94], which perfectly suits for REC and its activities as a part of smart cities development which

encompasses both green and digital transition.
Of course, it is trustworthy to refer to environmental principles, but the core aim of this paper is that the sincere cooperation could act in a substantial way as to push the administrative action to be effective, matching its results[95].
Specifically, according to articles 16 and art. 22 (6) of Directive 2018/2001/EU, Member States may provide in the enabling regulatory framework, that these communities are open to cross-border participation. Also significant is Recital 22 hoping a cross-border support for renewable energy not affecting national support schemes in a disproportionate manner.
As already mentioned, all these efforts are aimed at the transition to a more equitable, sustainable society, where present and next generations can enjoy a quality environment: shortly, to pave a better future for the future generation[96].
On this purpose, insofar as climate change represents a natural and man-made catastrophe, it may represents a trigger for solidarity obligations under Article 222 TFEU[97]. This principle, as well experimented in the Covid health crisis[98] has often evolved to adapt to the needs of the moment and the risk society[99].
Moreover, solidarity is also a value that would be addressed to future generations in a *One Health* perspective, as an integrated approach to health which recognizes the health of humans, domestic and wild animals, plants, and the wider environment (including ecosystems and its sustainability) are closely linked and interdependent[100]. On this path it is worth to mention the principle of non-regression aimed at protecting the acquired level of environmental protection (in the perspective of climate neutrality) in order to allow for the protection of future generations too[101]. Actually, all these considerations aim to show how bet on renewable energy sources in smart cities means also pursuit sustainability goals. As a matter of fact, the application of principle of non-regression is not defined at the EU level, even though already recognized at national level by some Member States[102], it's far from being simple if we assume that the achievement environmental sustainability faces transnational context relying upon multilayered sources and complex interrelationship[103] among EU, Member States and Third countries. Therefore, being a source of inspiration[104], principle of sincere cooperation is helpful as to carry out a result-oriented administrative action fostering new experiment in administration activity.
It can be argued that all the measures adopted from current generations, under

the *Green Deal strategy*, are supposed to deeply consider the protection of future citizens, in an intergenerational perspective which aims to seriously tackle with climate neutrality, assuring a sustainable development. Therefore, REC would represent a specific tool which can pave the way to many other smarts means to support other protection requirements for citizens involved in energy market revision which also aimed at ensuring the affordability of supply for less advantaged people[105]. For these reasons, administrative activity dealing with REC must also be oriented towards the *effectiveness* of its action involving for sure the public interest of climate neutrality as specified in the *Green Deal* strategy. Meanwhile, it aspires to the satisfaction of citizens' needs, in a broader perspective embracing (among others) industrial policy and the market, that also looks to future generations. Clearly, principle of sincere cooperation pushes the administrative process, which enhance the development of REC[106] in a *smart sustainable city,* and steer the administrative procedure in a multilevel playing field.

1. This article elaborates the speech delivered by the Authors at the roundtable "*Charting the course towards smart cities*" at Charles University – Prague on last 11th October 2024. It represents also a deliverable of the Jean Monnet Module named "*Public Administrations in the EU Energy Policies and Communities (101175226-PAEPeC)*" ongoing at Department of Italian and Supranational Public Law of University of Milan. The idea here developed is the straightforward expression of a joint approach of the two Authors, through the interaction of points of view. The parts of the text, in each case, can be attributed as follows: Alessia Monica wrote §1; § 3; §4; Leonardo Scuto wrote §2; 2.1; 2.2.
2. The definition of Smart City, in the EU and national perspective, is not univocal and is still in progress. See, among others, J.B. Auby, *Droit de la ville. Du fonctionnement juridique des villes au droit à la Ville*, II Ed., LexiNexis, Paris, 2016. M. Caporale, *El régimen de las smart cities en Italia*, in F. García Rubio (ed.), *Las nuevas perspectivas de la ordenación urbanística y del paisaje: smart cities y rehabilitación Una perspectiva hispano-italiana*, Fundación democracia y Gobierno LocaL, Barcelona, 2017, pp. 205-220.
3. Definition of REC is better reported in the note No. 42 *infra*.
4. C. Lauri, *L'ordinamento giuridico della smart city*, Jovene, Napoli, 2023, p. 44.
5. L. Diestelmeier, *The Role of Energy Communities in Facilitating Sustainable Energy Democracy*, in R. Fleming, K. Huhta, L. Reins (ed.), *Sustainable Energy Democracy and the Law*, Brill, Leiden, 2021, p. 124.
6. Regarding the functional legitimacy of EU and its administration see M. P. Chiti, *La legittimazione per risultati dell'Unione europea quale "comunità di diritto amministrativo"*, in *Rivista italiana di diritto pubblico comunitario*, 2, 2016, pp. 397-419.

7. Paradigm, according to ancient Greek is composed of preposition παρα- «para-» and the verb δείκνυμι «show» and it is a synonymous of "model of declination"; "example".
8. C. Lauri, *L'ordinamento giuridico della smart city*, cit., p. 49. See also G. Carullo, *Artificial Intelligence in smart cities for a dynamic and adaptive governance model*, in J.B. Auby (ed.), *Le future du droit administrative*, Lexis Nexis, Paris, 2019, pp. 365-376.
9. The University of Vienna tailored a functionalised concept of smart city developed on six main axis such as «*smart cities, smart economy, smart mobility, smart environment, smart people, smart living, smart governance*» https://www.smart-cities.eu/model.html.
10. A. Barone, *Il diritto del rischio*, Giuffrè, Milano, 2006, p. 37.
11. «*Smart city is an order made between orders*», C. Lauri, *L'ordinamento giuridico della smart city*, cit., p. 93.
12. «*Smart city is a system of systems*»: M.J. Madison, M.R. Sanfilippo, B.M. Frischmann, *Smart Cities and Knowledge Commons*. in M.J. Madison, M.R. Sanfilippo, B.M. Frischmann (ed.), *Governing Smart Cities as Knowledge Commons*, Cambridge University Press, Cambridge, 2023, p. 12.
13. R. Cavallo Perin, G. M. Racca, *Smart Cities for an Intelligent way of Meeting Social Needs*, in J.B. Auby, (ed.), *Le future du droit administrative*, cit., p. 437.
14. M.J. Madison, M.R. Sanfilippo, B.M. Frischmann, *Smart Cities and Knowledge Commons*, cit., «*The emphasis on public sector actors can be misleading. By design, smart city practices can be anchored in private sector activity, and they're intended to shape personal and private lives as well as systems of public administration*», p. 12.
15. According to French language, it is also used the expression "*ville intelligente*" which is mainly characterised by the increased production and use of data that aims to enable the management of new urban environments, in a connected and digital way. M. De Gioia, *Ville intelligente et médiation: réflexions linguistiques*, in *Cross-Media Languages Applied Research, Digital Tools and Methodologies*, 2, 2024, p. 21.
16. See Article 15., c.3 of Directive 2018/2001/EU.
17. I. Bouhadana, *The New Concept of smart Green Cities and Communities*, in G. de Jesús Sierra Cadena (cord.), *Derecho Administrativo y Ciudades Inteligente*s, Editorial Universidad del Rosario, Bogotà, 2021, p. 117.
18. J. Ziller, *Advance Introduction to EU Law*, Elgar, Cheltenham, p. 50.
19. Referring to sustainable development need to quote the report of the United Nation, World Commission on Environment and Development of 1987 entitled *Our common future* (https://digitallibrary.un.org/record/139811?v=pdf). In the EU Law, sustainable development is codified in the art. 3 (3) of TFEU and art. 11 TFEU. Actually, sustainable development, as a dynamic concept, is considered the development that meets the needs of the present without compromising the ability of future generations to meet their own needs. See *Agenda 2030 for Sustainable development* setting 17 goals (https://sdgs.un.org/goals).
20. See *above* note n. 19.
21. P. D. Cameron, *The consumer and the internal market in energy,* in *European law review*,

1 2006, pp. 114-124. According to the Author, among many benefits for the consumer experimenting more competition in the market since Directive 96/92/CE concerning common rules for the internal market in electricity, it is worthwhile the lowering of energy prices.

22. Since *Costa v. Enel* (Court of Justice, judgment, 15 July 1964, case 6/64, ECLI:EU:C:1964:66, concerning the nationalisation of the Italian electricity sector by Law No. 1643/1962 and well-known for the debate on the primacy principle, the governance of the energy sector has been an issue often debated in Courts. Specifically, in *Comune di Almelo,* (Court of Justice, judgment 27 April 1994, C-393/92, ECLI:EU:C:1994:171) the Court defined the energy as a "good": «*In Community law, and indeed in the national laws of the Member States, it is accepted that electricity constitutes a good within the meaning of Article 30 of the Treaty. Electricity is thus regarded as a good under the Community's tariff nomenclature (code CN 27.16). Furthermore, in its judgment in Case 6/64 Costa v ENEL [1964] ECR 1141 the Court accepted that electricity may fall within the scope of Article 37 of the Treaty*», para 28.
23. EU Commission, *The European Green Deal*, COM (2019) 640 final, 11 December 2019.
24. «*A smart sustainable city is an innovative city that uses ICTs and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects*».
25. Art 9 Cost., A. Lauro, *Dalla tutela ambientale in Costituzione alla responsabilità politica (anche) verso le future generazioni? Detti e non-detti di un principio di origine giurisprudenziale*, in *Rivista di BioDiritto*, 2, 2022. For a general overview see A. Donati, *I principi a tutela delle generazioni future nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, XIX, 2024, pp. 65-85.
26. P. Lombardi, *New challenges in the Evaluation of Smart Cities*, in *Network Industries Quarterly*, 3, 2011, p. 9.
27. The transition towards the use of renewable energy sources constitutes one of the key elements in the EU's fight against climate change, as highlighted, among others, in the report on the "*State of the Energy Union 2022*", referred to in the Report from the Commission to the European Parliament of 18 October 2022, COM(2022) 547 final. Over the years, in fact, the EU legislator has embarked on an important path of transforming general EU policy in a sustainable direction, in line with international commitments (e.g., *Paris Agreement on Climate Change* which was the first universal and legally binding global climate agreement, ratified by the EU on 5 October 2016). With this in mind, the Commission adopted in 2016 a set of legislative proposals on '*Clean Energy for All Europeans package*' (better known as the "*Clean Energy Package*"), aimed at renewing EU energy law.For a full analysis in this sense, please refer to A. Grignani, *Le comunità di energia rinnovabile: utile risorsa per il contrasto alla povertà energetica*, in *Ambiente e sviluppo*, 2, 2022, p. 113.
28. With reference to the notion of "energy consumer", see L. Ruggeri, *La protezione del*

consumatore energetico nel quadro regolatorio italo-europeo, in S. Monticelli, L. Ruggeri (a cura di), *La via italiana alle comunità energetiche*, Edizioni Scientifiche Italiane, Napoli, 2022; V. Caforio, *Il consumatore energetico*, in S. Monticelli, L. Ruggeri (a cura di), *La via italiana alle comunità energetiche*, cit., p. 83; C. Acosta, M. Ortega, T. Bunsen, et. al., *Facilitating energy transition through energy commons: an application of socio-ecological systems framework for integrated community energy systems*, in *Sustainability*, 2018, p. 366; L. Rossi Carleo, *Il diritto dei consumi in Italia,* in L. Rossi Carleo (ed.), *Diritto dei consumi*, Giappichelli, Turin, 2015.

29. On this topic, among others, see E. Cusa, *Sviluppo sostenibile, cittadinanza attiva e comunità energetiche*, in *Orizzonti del Diritto Commerciale*, 1, 2020; R. Miccù, M. Bernardi, *Premesse ad uno studio sulle Energy communities: tra governance dell'efficienza energetica e sussidiarietà orizzontale*, in *Federalismi.it*, 4, 2022; E. Ferrero*, Le Comunità Energetiche: ritorno a un futuro sostenibile*, in *Ambiente & Sviluppo*, 2020, p. 677; C. Bevilacqua, *Le Comunità Energetiche tra governance e sviluppo locale,* in *Amministrazione in cammino*, 1, 2020.
30. A. Coiante, *Le comunità energetiche rinnovabili nel quadro giuridico europeo e nazionale: un'occasione per ripensare l'ambito di operatività del silenzio assenso in materia di incentivi economici per la produzione di energia*, in *Diritto e Società*, 4, 2022, p. 735 (the translation is made by the Authors).In the same sense, see A. Persico, *Le comunità energetiche e il ruolo sussidiario delle pubbliche amministrazioni territoriali. Moduli e strumenti a disposizione delle pubbliche amministrazioni per favorire la costituzione e le attività delle comunità di energia rinnovabile,* in *Ambiente-Diritto.it*, 2, 2022.
31. Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on "*the promotion of the use of energy from renewable sources*".
32. Legislative Decree of 8 November 2021, No. 199 on "*Implementation of Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources*".
33. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on "*common rules for the internal market for electricity and amending Directive 2012/27/EU*".
34. Italian Legislative Decree of 8 November 2021, No. 210 on "*Implementation of the EU Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 concerning common rules for the internal market in electricity and amending Directive 2012/27/EU, as well as laying down provisions for the adaptation of national legislation to the provisions of EU Regulation 943/2019 on the internal market in electricity and EU Regulation 941/2019 on risk preparedness in the electricity sector and repealing Directive 2005/89/EC*".
35. This concept has been defined by Art. 2(11) of Directive UE/2019/944, according to which it is a legal entity that «*(a) is based on voluntary and open participation and is effectively controlled by members or shareholders that are natural persons, local authorities, including municipalities, or small enterprises; (b) has for its primary purpose to provide*

environmental, economic or social community benefits to its members or shareholders or to the local areas where it operates rather than to generate financial profits; and (c) may engage in generation, including from renewable sources, distribution, supply, consumption, aggregation, energy storage, energy efficiency services or charging services for electric vehicles or provide other energy services to its members or shareholders».In this regard, see M. F. Lucente, *La comunità energetica dei cittadini*, in *La via italiana alle comunità energetiche*, in S. Monticelli, L. Ruggeri, *La via italiana alle comunità energetiche*, cit., p. 49.

36. Further fundamental definitions, relevant to the matter at stake, are that of "self-consumers of renewable energy acting individually" and that of "self-consumers of renewable energy acting collectively". On this point, see §2.2. below.
37. In this regard, among others, see E. Cusa, *Il diritto dell'Unione europea sulle comunità energetiche e il suo recepimento in Italia*, in *Rivista trimestrale di diritto dell'economia*, 2, 2020, p. 287.
38. It should be noted in this respect that the REC must be controlled by shareholders or members located in the vicinity of the renewable energy production facilities owned and developed by the REC itself. In contrast, this requirement does not seem to apply to CECs.
39. In this regard, see Recital 71 of RED II, according to which «*The specific characteristics of local renewable energy communities in terms of size, ownership structure and the number of projects can hamper their competition on an equal footing with large-scale players, namely competitors with larger projects or portfolios. Therefore, it should be possible for Member States to choose any form of entity for renewable energy communities, provided that such an entity may, acting in its own name, exercise rights and be subject to obligations. To avoid abuse and to ensure broad participation, renewable energy communities should be capable of remaining autonomous from individual members and other traditional market actors that participate in the community as members or shareholders, or who cooperate through other means such as investment. Participation in renewable energy projects should be open to all potential local members based on objective, transparent and non-discriminatory criteria. Measures to offset the disadvantages relating to the specific characteristics of local renewable energy communities in terms of size, ownership structure and the number of projects include enabling renewable energy communities to operate in the energy system and easing their market integration. Renewable energy communities should be able to share between themselves energy that is produced by their community-owned installations. However, community members should not be exempt from relevant costs, charges, levies and taxes that would be borne by final consumers who are not community members, producers in a similar situation, or where public grid infrastructure is used for those transfers*».
40. On this concept see M. Meli, *Autoconsumo di energia rinnovabile e nuove forme di energy sharing*, in *Nuove leggi civ. comm.*, 3, 2020, p. 633; M.A. Heldeweg, S. Saintier, *Renewable energy communities as "social-legal institution": a normative frame for energy decentralisation*?, in *Renewable and Sustainable energy reviews*, 1, 2020, p. 119; A. Maestroni, M. De Focatiis (ed.), *Politica energetica, regolazione e mercato. Il nuovo diritto*

dell'energia tra libertà e limitazioni concorrenziali e ambientali, Giuffrè, Milan, 2012.

41. Recital No. 43 of RED II.
42. This means that, according to the applicable the EU legislation, as considered in this paper, RECs may include a wider range of actors who are able to participate. In this regard, a confirmation of the above is offered by the definition set forth in Article 2, par. 16 of the RED II, pursuant to which 'Renewable Energy Community means a legal entity «*(a) which, in accordance with the applicable national law, is based on open and voluntary participation, is autonomous, and is effectively controlled by shareholders or members that are located in the proximity of the renewable energy projects that are owned and developed by that legal entity; (b) the shareholders or members of which are natural persons, SMEs or local authorities, including municipalities; (c) the primary purpose of which is to provide environmental, economic or social community benefits for its shareholders or members or for the local areas where it operates, rather than financial profits*».
43. On this topic, among others, see the various contributions in L. Cuocolo, P. P. Giampellegrini, O. Granato, *Le comunità energetiche rinnovabili*, Egea, Milano, 2023.
44. With reference to the previous "transitional regulation", implemented by the national legislator pending the full transposition of the relevant Directives, Article 42-*bis* of Law Decree No. 162/2019 is of vital importance. For a full analysis in this sense, see G. Argirò, *L'evoluzione del quadro normativo europeo e italiano sulle comunità energetiche rinnovabili*, in L. Cuocolo, P. P. Giampellegrini, O. Granato, *Le comunità energetiche rinnovabili*, cit., p. 19.
45. Reference is made to the (i) ARERA Regulation named "*Testo Integrato Autoconsumo Diffuso – TIAD*" (hereafter, "TIAD"), (ii) MEES Decree No. 414 of 7 December 2023, and (iii) GSE Operating Rules of April 2024 named "*Decreto CACER e TIAD – Regole operative per l'accesso al servizio per l'autoconsumo diffuso e al contributo PNRR*".
46. It should be noted that the National Recovery and Resilience Plant, M2C2 – "*Renewable Energy, Hydrogen, Grid and Sustainable Mobility*", envisages 2.2, billion euros specifically for the promotion of renewable energy source for RECs and for self-consumption. The aim is to transpose the RED II Directive more effectively.
47. Provision has also been made for the possibility of extending the REC to existing RES-fuelled power generation plants, i.e. those that came into operation before the decree came into force, as long as they do not exceed 30 per cent of the total power output of the community.
48. Italian NRRP (*Piano Nazionale di Ripresa e Resilienza*), https://www.italiadomani.gov.it/content/sogei-ng/it/en/home.html.
49. See in particular what is specified in paragraph 1(e) of the regulatory provision in question, pursuant to which «*in implementing the measures Mission 2, Component 2, Investment 1.2 "Promotion of renewables for energy communities and self-consumption", criteria and procedures are defined for the granting of interest-free financing of up to 100 per cent of eligible costs, for the development of energy communities, as defined in Article 31, in small municipalities through the construction of RES production plants, including those combined*

with energy storage systems. The same decree defines the conditions of cumulability with the tariff incentives under Article 8».

50. See, among others, M. Bernardi., L. Tricarico, *Commoning e comunità energetiche: approcci di citizen science nella produzione distribuita d'energia*, in *Munus*, 3, 2021; C. Bevilacqua, *Le Comunità Energetiche tra governance e sviluppo locale*, in *Amministrazione in cammino*, 1, 2020.
51. With reference to the incentive scheme, it is useful to bear in mind what is indicated – as to definitions – by the Ministerial Decree at stake, and in particular by Article 2 under which the «*self-consumption configurations for sharing renewable energy*» are represented by one of the configurations referred to in letters e), f) and g) of the same rule, which use the existing distribution network to share the energy produced by renewable energy plants, and in particular:e) Individual Remote Renewable Energy Self-Consumption Systems: «*systems that provide for the remote self-consumption of renewable electricity by an individual end-customer, without the use of a direct line, using the existing distribution network to connect production sites and consumption sites, pursuant to Article 30, paragraph 1, letter a), number 2.2 of Legislative Decree No. 199 of 2021*». This is the Autoconsumer Distance;f) Collective self-consumption systems from renewable sources: «*systems implemented by groups of self-consumers acting collectively pursuant to Article 30(2) of Legislative Decree No. 199 of 2021*». This refers to the group of self-consumers;
g) Renewable Energy Communities: «*systems implemented by end customers pursuant to Article 31 of Legislative Decree No. 199 of 2021*». These are CERs, in fact (the translation is made by the Authors).
52. On this topic, among others, see U. Tedeschi, P. De Angelis, *Project financing: uno strumento "alternativo" per finanziare grandi opere*, in *Amministrazione&Finanza*, 15-16, 1998, p. 48; A. Ponzio, A. Palumbo, *I rischi climatici e la loro rilevanza nell'informativa finanziaria*, in *Bilancio e revisione*, 3, 2024, p. 19.
53. The translation is made by the Authors, in Italian "*soggetto di diritto autonomo*".
54. Enacting «*Urgent provisions for the implementation of the National Recovery and Resilience Plan (NRRP) and the National Plan for Complementary Investments to the NRP, as well as for the implementation of cohesion policies and the Common Agricultural Policy*» (the translation is made by the Authors).
55. The translation is made by the Authors, in Italian "*associazioni con personalità giuridica di diritto privato".*
56. On this point, see Study No. 38-2024/I prepared by the National Council of Notaries, and in particular by E. Cusa, *Le incentivate comunità energetiche rinnovabili e il loro atto costitutivo*, in *CNN Notizie*, 57, 2024, p. 1.
57. In this regard, it is worth noting the provisions of Article 32(b)(1) of Legislative Decree No. 199/2021, pursuant to which the end customers organised in a REC «*may withdraw at any time from the self-consumption configuration, without prejudice to any fees agreed upon in the event of early withdrawal for the sharing of the investments incurred, which must in any event be fair and proportionate*» (the translation is made by the Authors).

58. Recital 43, Directive 2019/944/EU.
59. See also art. 13 (2) TEU.
60. L. Parona, *Addressing the interplay between competition law and data protection law in the digital economy through administrative cooperation: the CJEU judgment in the Meta Platforms case*, In *Italian Journal of Public Law*, 1, 2024, p. 254.
61. M. Lottini, *From 'Administrative Cooperation' in the Application of European Union Law to 'Administrative Cooperation' in the Protection of European Rights and Liberties*, in *European Public Law*, 2012, 1, pp. 127-128.
62. Commission Recommendation 2009/524/EC of 29 June 2009 on measures to improve the functioning of the single market.
63. E. Chiti, *Managing the ecological transition of the EU: The European Green Deal as a regulatory process*, in *CMLR*, 1, 2022, pp. 39-42.
64. D. Bevilacqua, E. Chiti, *Green deal. Come costruire una nuova Europa*, il Mulino, Bologna, 2024, p. 48.
65. D. Sorace, *Il servizio d'interesse economico generale dell'energia elettrica in Italia tra concorrenza ed altri interessi pubblici*, in *Diritto pubblico*, 3, 2004, p. 1010.
66. 197 TFEU. See, among others, F. Lafarge, *Administrative cooperation between member states and implementation of EU law*, in *European public law*, 4, 2010, pp. 597-616.
67. Optional cooperation mechanism between Member States were already present since the Directive 2009/28/CE as to facilitate the achievement of set target. See, M. M. Roggenkamp, C. Redgwell, A. Rønne, I. Del Guayo, *Energy Law in Europe*, III Ed., Oxford university Press, Oxford, 2016, p. 325.
68. R. Lanceiro, *Mechanisms of Transnational Administrative Cooperation Under the EU Environmental La*w, in *Italian Journal of Public Law*, 2024, n. 2, p. 343.
69. Recital 9 Directive 2019/944/EU.
70. C. Harlow, R. Rawlings, *Process and Procedure in EU Administration*, Hart Publishing, Oxford, 2014, p. 40.
71. Court of Justice, 8 October 2020, case C-514/19 *Union des industries de la protection des plantes,* ECLI:EU:C:2020:803, para 49.
72. A. Giordano, *Le comunità energetiche nell'era della sostenibilità*, in *CERIDAP*, Special Issue 3, 2024, pp. 39-55.
73. P. Lehmann, E. Gawel, *Why Should Support Schemes for Renewable Electricity Complement the EU Emissions Trading Scheme?*, in *Energy policy* 52, 2013, pp. 597–607.
74. C. Cambini, A. Manganelli, A. Nicita, G. Napolitano (ed.), *Economia e diritto della regolazione*, Il Mulino, Bologna, 2024, p. 84.
75. Article 1 Directive 2019/944/EU.
76. Specifically, it is a duty of regulatory authorities of Member States cooperating in regard to cross-border issues with ACER. See articles 58 and 59 Directive 2019/944/EU.
77. F. Battaglia, *Il principio di leale cooperazione nel Trattato di Lisbona. Una riflessione sulle vicende legate al recesso del Regno Unito dall'Unione europea*, in *Federalismi.it*, 19, 2020, p. 33.

78. Court of Justice, 8 October 2020, case C-514/19, *Union des industries de la protection des plantes*, cit., para 50.
79. P. Marzaro, *Leale collaborazione e raccordo tra Amministrazioni; su un principio del sistema a margine delle 'riforme Madia,* in *Federalismi.it*, 23, 2017, p. 13 (the translation is made by the Authors).
80. *Id*., 13 (the translation is made by the Authors).
81. See, Court of Justice, 25 May 1982, Case 96/81 *Commission v. Netherlands*, ECLI:EU:C:1982:192, para 7.
82. Regulation (EU) 2018/1999 of the European Parliament and of the Council of 11 December 2018 on the Governance of the Energy Union and Climate Action.
83. G. Corso, M. De Benendetto, N. Rangone, *Diritto amministrativo effettivo*, Il Mulino, Bologna, 2022; A. Monica, *Open Data and Composite Procedures: Strengthen the Quality and the Effectiveness of Administrative Activity*, in *AUC IURIDICA*, 2, 2024, p. 50.
84. G. Balduzzi, *Cambiamento istituzionale e organizzativo: verso un approccio multidimensionale*, in D. Fromage (ed.) in *Jacques Ziller: an European scholar*, EUI, Fiesole, 2022, pp. 202-215.
85. D.U. Galetta, H. Hofmann, J.P. Schneider, *Information Exchange in European Administrative Union*, in *European Public Law*, 20, 2024, p. 89.
86. COM (2022), 289 def, *Strategic Foresight Report Twinning the green and digital transitions in the new geopolitical context*.
87. E Chiti, B. Marchetti, N. Rangone, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in *BioLaw Journal*, 2, 2022, p. 500.
88. H. Hofmann, *Composite Decision Making Procedures in EU Administrative Law*, in H. Hofmann, A. H. Turk (ed.), *Legal Challenges in EU Administrative Law*, Edwar Elgar, Cheltenham, 2009, p. 136.
89. See art. 28 Directive 944/2019/EU.
90. L. De Lucia, *Strumenti di cooperazione per l'esecuzione del diritto europeo*, in *L'amministrazione europea e le sue regole*, Il Mulino, Bologna, 2015, p. 193.
91. See Italian l. 241/90, art. 1, par. 1-ter.
92. Smart cities show new experiments in local governance relying also on public-partnership to implement new strategies opening also new legal challenges. «*Actors are pushing the boundaries of collaboration and consultation, beside competition, even further than in a traditional public private partnership to create a sense of community around a local project, connected to a wider web of European cities*», in Y. Marique, S. Van Garsse, *Setting up public- private partnerships in smart cities*, in J.B. Auby (ed.), *Le future du droit administrative*, Lexis Nexis, Paris, 2019, p. 362.
93. For example, both for plants that transfer all the energy produced to the electricity grid, and for plants in partial transfer combined with self-consumption, the local authority must activate an energy management contract in order to receive the value of the energy fed into the grid. See Vademecum ANCI per i comuni, April 2024, https://www.anci.it/wp-content/uploads/CACER_Vademecum_ANCI-240412-corrett

o-stampa.pdf.

94. F. Lafarge, *Administrative cooperation between member states and implementation of EU law*, cit. p. 611.
95. Italian Constitutional Court, judgment 27 July 1992, n. 379.
96. R. Bifulco, *Diritto e generazioni future*, Franco Angeli, Milano, 2008; A. Donati, *I principi a tutela delle generazioni future nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 1, 2024, pp. 65-85.
97. A. Donati, *I principi a tutela delle generazioni future nel diritto dell'Unione europea*, cit., p. 79.
98. EU Commission, *Europe's moment: Repair and Prepare for the Next Generation*, COM (2020) 456, 27 May 2020.
99. Court of Justice, judgment 16 February 1982, case 276/80 *Ferriera Padana*, ECLI:EU:C:1982:57, para 27; Court of Justice, judgment, 5 May 2022, C-405/20 *BVAEB*, ECLI:EU:C:2022:347, para 56. Substantially, the CJEU is called upon to examine if some '*social balancing'* tools, affecting companies, firms or individuals, which are intended to prevent an excessive large gap opening up between different groups in the same sector, are not discriminatory measures.
100. A. Latino, *Il paradigma One Health nell'ordinamento internazionale: un'analisi critica di origini, protagonisti, strumenti normativi*, in *Corti supreme e salute*, 3, 2022, pp. 779-808.
101. M. Prieur, *L'émergence du principe de non régression ou l'illustration du rôle de la doctrine dans la création du droit de l'environnement*, in *Rivista Quadrimestrale di diritto dell'ambiente*, 2, 2021, p. 27.
102. M. Calabro, *L'ambiente quale diritto fondamentale a titolarità diffusa*, in *Persona e Amministrazione*, 2, 2024, 501-536.
103. M. Antonioli, *Lessons on Sustainable Development in EU Law*, Aracne, Roma, 2020, p. 19.
104. C. Harlow, R. Rawlings, *Process and Procedure in EU Administration*, cit., p. 41.
105. C. Armeni, *What justice? The scope for public participation in the European Union Just Transition'*, in *Common Market Law Review*, 4, 2023, pp. 1027-1054.
106. Recital 39 Directive 2018/2001/CE.

Deployment of AI in public transport in smart cities as a challenge for tort law

Marianna Novotná, Veronika Zoričáková

DOI: 10.13130/2723-9195/2025-2-43

Una caratteristica tipica delle tecnologie che utilizzano forme di controllo autonome è la loro crescente complessità derivante dall'aumento del grado di automazione che, in relazione al processo del loro utilizzo nella vita quotidiana, presenterà nuovi rischi che aumentano soprattutto quando i sistemi autonomi sono utilizzati nel trasporto pubblico urbano, dove è più alto il rischio di causare danni alla salute e alla vita di un gran numero di persone contemporaneamente. Questi rischi sono legati alla questione del funzionamento di un regime di responsabilità civile che rifletta la distribuzione dei rischi in relazione all'utente diretto, al produttore o all'operatore del sistema autonomo attraverso lo standard di cura previsto. Il presente articolo mostra in quale direzione e su quali basi si potrebbero fare considerazioni nel definire il livello di cura previsto e in quale misura è applicabile anche l'attuale impostazione dei rapporti di responsabilità. Infine, verranno illustrate le modifiche legislative pilota in alcuni Paesi in materia di responsabilità per i veicoli autonomi, insieme al regime della nuova direttiva sulla responsabilità del prodotto per gli sviluppatori di software.

A typical feature of technologies using autonomous forms of control is their increasing complexity resulting from the increasing degree of automation, which, in relation to the process of their use in everyday life, will present new risks that mainly increase when autonomous systems are used in urban public transport, where there is a higher risk of causing harm to the health and life of a large number of people at once. These risks are linked to the issue of the functioning of a civil liability regime that would reflect the distribution of risks in relation to the direct user, manufacturer or operator of the autonomous system through the expected standard of care. The paper shows in which direction and on what basis considerations could be taken when defining the expected level of care and to what extent the current setting of liability relationships is also applicable. Finally, we will present pilot legislative changes in some countries

regarding liability for autonomous vehicles and outline the new Product Liability Directive regime for software developers.

Summary: 1. Initial remarks.- 2. Planned and implemented autonomous public transport projects.- 3. Risks Associated with the Use of Autonomous Public Transport Systems and Their Allocation.- 4. Liability for damage caused by autonomous public transport systems and potential liable persons.- 4.1. Fault-based unlawful conduct as a legal basis for damage attribution.- 4.2. Attribution of liability based on grounds other than fault (liability of the operator, producer, and developer of autonomous public transport systems).- 5. New horizons and upcoming trends in recent legislation to address the issues of liability for autonomous systems.- 6. Conclusion.

1. Initial remarks

As we look towards a future where vehicles can see[1], think, and learn[2], seamlessly integrating into the framework of smart cities as autonomous public transport – this evolution prompts us to carefully address important liability issues alongside the technical and technological challenges we face, including the collection, processing, and protection of data, protection of personality rights of all individuals involved in transportation[3], and significant ethical aspects[4].

It is precisely the question of liability for damage caused by various roboshuttles, autonomous buses, or self-driving trams, where human influence in driving will be eliminated or reduced to a minimum, that must not be overlooked when considering smart cities. This applies in cases where such vehicles cause harm to transported passengers (e.g., injury to life, health, or property) or to individuals who are not passengers but suffer damage caused by autonomous public transport systems.

Autonomous vehicles are regarded as one – if not the main – possible technology that is to be a part of multi-faceted approach to support the achievement of smart city goals[5]. The autonomous vehicles are hence one of the main "building blocks" of smart cities and are simultaneously a staple symbol of establishing smart urbanisation and innovation in general.

2. Planned and implemented autonomous public transport projects

There are numerous projects already implemented in different areas of the world when it comes to autonomous public transport. In 2016 in Australia, the first live test of the autonomous bus RAC Intellibus was launched in the city of Perth. This bus operated regularly and concluded its service in 2023 with no caused accidents. It was capable of transporting up to 15 passengers, with a maximum speed of 45 km/h[6].

In 2017, the first trial ride of the experimental Future Bus, equipped with CityPilot technology from Mercedes-Benz took place in the Netherlands. This demonstration proved that autonomous public transport indeed can offer enhanced safety, fuel savings, and improved comfort. These rides were conducted with a driver present, as required by regulations, and were generally deemed successful[7].

Also in 2017, Techbox reported on a hybrid of a train and a bus developed in China. The concept, known as Autonomous Rail Rapid Transit (ART), represents a connected convoy of buses capable of running along a designated route without a driver[8].

In 2018, the first self-driving tram was tested in Germany at the InnoTrans 2018 trade fair. This tram, called Siemens Combino, conducted a test ride without passengers in a regular traffic[9]. The tram utilized elements of artificial intelligence, although a human operator was still present. During the test ride, various simulated emergency situations were carried out, and the test was generally considered successful[10]. The city of Hamburg has the potential to become a pioneer in autonomous transport in Europe as the first tests of autonomous buses took place in 2019, and starting next year, the city will continue testing additional autonomous vehicles[11]. Later on in 2023, MAN announced that it had entered into a collaboration with Mobileye, a subsidiary of Intel. Their first joint objective is to launch the pilot operation of the first automated urban bus with a safety driver, starting in 2025, as part of the newly announced research project MINGA in Munich[12].

In 2019, Volvo, in collaboration with Nanyang Technological University, launched a pilot project for the world's first fully autonomous electric bus in

Singapore. This was the Volvo 7900 Electric, a fully electric bus with a capacity of nearly 80 passengers[13]. The trial operation concluded in 2023[14]. Again in 2019, Volvo Buses demonstrated an autonomous version of its 7900 Electric urban bus in Sweden. The demonstration took place in collaboration with Keolis, near Gothenburg. The test operation was, too, successful[15].

Huge success in the area of smart cities' public transport was reported from the United Kingdom in 2022. Fusion Processing announced the commencement of testing for the Dennis Enviro200 autonomous bus as part of the CAVForth project, which had been under development since 2020 and its members claim that one of their primary motivations is safety, as up to 86% of traffic accidents on the roads of the United Kingdom are caused in some way by human error. The bus has a capacity of up to 36 passengers and operates along a route of approximately 22 km[16]. This bus is still in operation and has even won the "Self-Driving Industrial Vehicle of the Year" award[17]. However, the first fully autonomous bus service in the United Kingdom was launched in Scotland in 2023. It is described as the most ambitious and complex autonomous bus pilot project in the world and these buses, too, are a part of the CAVForth project implementation. The second phase of the project is known as CAVForth II, which will extend the current route by an additional 5 miles. This phase is set to begin after the completion of the first phase, with a planned continuation at least until March 2025[18].

Norway launched the operation of autonomous buses in the city of Stavanger. This is not a pilot test but a fully operational bus service[19]. In 2022 the e-Atak electric bus was introduced as an autonomous vehicle that reaches speed of up to 50 km/h and can transport up to 52 passengers. The bus is capable of performing autonomous tasks – previously carried out by a human driver – both day and night, such as stopping at bus stops, opening doors for boarding and alighting, and similar functions[20].

In the field of public transport particularly in Slovakia, data collection for the development of autonomous bus control systems was conducted in Bratislava as part of the Pilot Project for Smart Mobility of the Future in the first half of 2021. This project was implemented at the Slovak University of Technology with cooperation of the Žilina University[21]. The data collection was carried out using a bus equipped with sensors (cameras, radars), which gathered data from real-

world traffic. These will be used in the development of autonomous bus control systems to be implemented in near future through a new platform[22].
This new platform, which is also a multi-sector interest association of legal entities, Smart Mobility Slovakia, is dedicated to creating conditions and actively advocating for the development of smart mobility[23]. This shall include preventing traffic jams, addressing parking issues, reducing emissions, as well as supporting sustainability. Even though the development is not yet implemented in day-to-day life of public transport, due to leading automotive manufacturers focusing on research and development in the concept of autonomous mobility there is high potential for autonomous control in public transport in near future.
When it comes to plans for implementing semi-autonomous and autonomous public transport in EU, according to the President of the German Federal Motor Transport Authority (KBA), Richard Damm, a significant breakthrough in autonomous transport is expected within the next few years. He states that by 2026 or 2027 at the latest the first autonomous buses will be operating in European cities transporting real passengers. According to him, "robot buses" are sufficiently safe, with only minimal residual risks remaining. He anticipates that within 5 to 10 years, autonomous transport, including buses and freight vehicles without drivers, will be used widely and regularly[24].
In Hong Kong it is expected that the largest autonomous bus transport system will be operational by the end of 2025. The total route length is expected to be approximately 850 meters, with a travel time of under 3 minutes. Each bus can carry a maximum of 16 passengers per trip. The initial goal of the system is to achieve a transport capacity of about 500 passengers per hour, with each bus operating a one-way route[25].
These were just a fraction of all the innovations that consecutively give life to plans and ideas that were not that long ago a mere uncertain future possibility. Autonomous public transport is not just an intangible concept anymore but is slowly but steadily becoming a part of our everyday lives. This naturally comes hand-in-hand with new challenges to civil liability when it comes to possible risk of harms caused by these new integrated systems not controlled by a human driver.

3. Risks Associated with the Use of Autonomous Public Transport Systems and Their Allocation

Since civil liability fundamentally rests on the principle of attributability of harm caused to a subject other than the injured party based on special attribution grounds, assessing liability for damages caused by autonomous public transport vehicles during their operation primarily depends on evaluating the presence of such grounds of attribution.

A defining characteristic – and a problematic aspect[26] concerning the attribution of harm –is that the autonomy granted to such systems for decision-making and action ultimately results in limited predictability and imprecise traceability of their conduct. Even the programmer cannot reliably anticipate what behavioural algorithms[27] the autonomous system may acquire through learning or how it will specifically react in particular situations.

Given that predictability plays a crucial role in tort law, the occurrence of harmful consequences under such circumstances raises legitimate questions regarding the legal nature of liability, the entity to which such harm can be attributed, the determination of causality[28] (particularly in cases involving the complex interconnectivity of cooperating systems), and related issues. These are primarily discussed in the context of civil liability[29] for damages caused, while the criminal law aspects of autonomous control systems[30] are currently less prominently emphasised).

The core consideration in defining liability for autonomous public transport systems lies in determining to whom the erroneous behaviour of a public transport vehicle can be attributed and devising mechanisms for allocating the risks associated with their development, production, operation, and use. This allocation must respect and balance the legitimate interests of the various stakeholders[31] involved in relationships related to autonomous control systems.

The technical and technological specifics associated with using autonomous urban public transport in smart cities introduce new and, to varying degrees, specific risks, even in legal assessments. Tort law's role is to determine how these risks will be allocated and who will primarily bear them in cases where damage arises within the operational scope of such an autonomous transport system.

Risks that are (or will be) relevant and necessarily factored into the framework for

their allocation are linked to the high degree of automation inherent in these systems. These risks may arise from algorithmic errors or malfunctions in hardware[32]. A critical risk factor within autonomous control systems is integrating computational control with components that, in the "real" world, can exhibit forceful effects[33] (whether due to their physical, chemical, or other properties). Such software and hardware integration can create distinct risks, mainly when a software error directly triggers mechanical hazards[34] – an issue particularly characteristic of autonomous vehicles. From a frequency perspective, mechanical impacts of hardware are more likely to cause harm to life or health than software errors alone.

Another critical factor influencing the legal liability assessment is the mobility of autonomous public transport systems. Unlike static systems, mobility increases the radius within which harmful consequences may occur. Furthermore, their operation outside laboratory or industrial environments and deployment into real public spaces heighten risks due to the greater likelihood of unpredictable situations that autonomous public transport vehicles may encounter[35]. This risk is further exacerbated by the increased intensity of interactions with people, as human behaviour is also inherently unpredictable to a certain degree. This aspect is even more pronounced in autonomous public transport systems than standard individual autonomous vehicles, as public transport inherently involves large numbers of passengers or goods.

The interconnection of various systems processing the data necessary for the operation of autonomous buses, trams or roboshuttles also significantly raises the risk of inaccurate data being transmitted within this shared network, potentially leading to incorrect situational assessments by these systems. The mutual interdependence of individual systems on the accuracy of data collection, evaluation, and processing represents a limiting factor for attributing such risks to specific entities involved in the operation of the overall system, primarily due to unclear causal relationships.

A specific, novel risk typical of autonomous systems arises from the fundamentally unpredictable behaviour of self-learning algorithms[36] – *i.e.*, the risk inherent in the autonomous nature of such public transport systems. Given the current state of scientific and technological knowledge, the unpredictability of autonomous systems' behaviour assesses the nature, scope, and frequency of

risk realisation for liability purposes relatively complex. It has not yet been conclusively demonstrated whether autonomous control systems are as reliable and safe as the currently used systems dominated by human factors or, conversely, whether autonomous systems are to be regarded as less or more secure[37].

This assessment of risks currently remains in the realm of expert estimations[38]. Nonetheless, with a certain degree of exaggeration, one might fully agree with Marc Andreessen, who stated in an interview with The New York Times, «*People are so bad at driving cars that computers don't have to be that good to be much better. Any time you stand in line at the D.M.V. and look around, you're like, Oh, my God, I wish all these people were replaced by computer drivers*»[39].

4. Liability for damage caused by autonomous public transport systems and potential liable persons

The "traditional" tort law theory operates with several concepts through which conclusions can be drawn regarding who may bear liability for damage caused and under what conditions. The following text outlines whether and to what extent these general principles of civil liability can also be applied to damage caused by autonomous public transport systems.

In general, two major categories of grounds can be identified for attributing liability for damage to a specific party:

1. The category of individuals associated with the source of danger encompasses persons that contribute to the creation, operation, or use of a particular source of danger and to whom the obligation to compensate for damage resulting from the realisation of risks associated with such a source of danger is attributed[40], irrespective of fault or unlawful conduct.

Liable persons under this framework may include those whose abstract or concrete risks are tied to these systems, who derive benefits from them, or who possess the capability to control and manage them. Theoretically, such persons could include the system's producer, developer, programmer, supplier, or operator. Additionally, there is the prospective question of whether liability could, in future, be attributed to the autonomous system itself[41].

2. The second category of persons involves subjects assessed based on whether

they adhered to a required standard of care. If such a standard is breached and the person's actions directly lead to damage, liability for damage caused can be attributed.

Balancing these various concepts should ultimately yield a set of responsible entities normatively obligated to bear the adverse consequences.

Unfortunately, traditional theories of liability attribution and risk distribution – such as the control of risk theory[42], the benefit from risk theory, or the increased risk theory[43] –encounter significant challenges when applied to autonomous systems. Autonomous systems are not programmed to perform specific activities; instead, they are designed to independently learn how to perform such activities, continuously generating their own code (program) independently of their original creator[44]. This self-learning process, influenced by internal and numerous external factors, significantly diminishes any party involved's ability to create, operate, or use these systems to control or manage them effectively.

This issue manifests in two dimensions:

a) based on the legislature's legal and policy decisions, a normative risk allocation involves determining which entity will be held liable for damage caused by an autonomous system and under what conditions such liability will be attributed;

b) formal fulfilment of liability prerequisites concerns the practical ability to meet and demonstrate fulfilling the prerequisites required for establishing liability[45].

The unique characteristics of autonomous systems, particularly their capacity for independent and evolving decision-making, make reconciling traditional liability frameworks with their application reality challenging. These complexities necessitate reevaluating how liability is assigned, and risks are distributed within the legal structures governing autonomous public transport systems.

4.1. Fault-based unlawful conduct as a legal basis for damage attribution

The fundamental basis for attributing liability for damages generally stems from the fault of the person who caused the harm, whether through negligence or intent. Negligence refers to behaviour where the individual, under the required standard of care appropriate for the specific case and circumstances, could have

identified and prevented the harmful outcome[46].

In the context of autonomous control systems, the applicability of the fault principle is significantly limited. The higher the degree of autonomy of the system, the less feasible it becomes to identify a subject whose fault can be linked to a harmful outcome.

Depending on the level of autonomy in a public transport vehicle requiring some interaction from the driver, liability may be considered if the driver fails to adhere to the expected standard of behaviour mandated for operating such a system. Since public transport drivers are typically employees of a transport company, most legal systems would apply vicarious liability provisions, potentially attributing liability to the employer for harm caused by the employee. The specifics of this principal-agent liability may vary across jurisdictions, with the employer potentially being held jointly or solely liable alongside the employee.

The limitation of this fault-based framework stems from the rising degree of autonomy, which results in fewer responsibilities for the driver in managing non-standard situations or system errors. Consequently, the question of the standard of care is closely linked to the extent of system automation. As automation grows, users and other involved parties have greater expectations that the system will independently recognise and mitigate risks without external human intervention.

A breach of the standard of care, relative to the degree of autonomy in an autonomous public transport system, could manifest in real-life scenarios such as a driver of a highly autonomous vehicle failing to intervene when the system either does not react or reacts improperly, or ignoring system prompts to take control in an unusual situation. Such a lack of cooperation between the driver and the system could result in driver fault and liability for damage[47].

This principle applies even without explicit legal provisions outlining the rights and duties of autonomous system users. In many legal systems, the obligations of an autonomous system driver can be derived from the general statutory duty of care to act in a manner that prevents harm. Courts evaluate whether the expected standard of care was upheld in a given context.

A breach of the standard of care might occur, for instance, if a bus driver engaged in activities incompatible with promptly taking control upon a system prompt[48], significantly delayed their response or failed to assume control after being alerted

by the autonomous system[49].

As the degree of autonomy increases, the role of the human factor diminishes, reducing the scope for claiming damages from the driver. This is because the system's operation, including its decision-making and execution, is governed by computer algorithms. Except for specific circumstances, it can be affirmed that the qualitative and quantitative standard of care expected of drivers of autonomous systems is lower than for non-autonomous systems[50]. Consequently, the range of cases involving exclusive driver liability diminishes, with driver liability often reduced to contributory negligence, potentially shared with the injured party.

Given that defects in autonomous systems may increasingly originate from the system's technical design, care responsibilities will likely shift to entities capable of addressing such obligations, such as producers and programmers[51].

The attribution of fault as a legal basis for liability may extend to producers of autonomous systems if they breach contractual or statutory obligations and cause harm through such breaches. For example, a producer may be liable for failing to recall an autonomous system upon discovering safety risks or for neglecting to address a known issue through software updates[52].

Technical standards provide a baseline for defining the obligations of producers, though these represent minimum safety benchmarks[53]. Additional standards are derived from scientific and technical advancements to ensure the level of protection aligns with the existing state of scientific knowledge and practical feasibility[54].

Producers of autonomous systems must protect users and third parties from risks arising from both proper and improper system use. Expected standards of care for producers include the safe development and production of the system, protection against unauthorised interference by users or third parties[55], adequate user instruction and information, fulfilling ongoing maintenance obligations (e.g., providing necessary software updates), and proactively responding to defects, such as recalling defective units.

If the autonomous driving system is a combination and cooperation of software and hardware, which autonomous public transport vehicles fulfil, it is questionable whether the hardware producer should also be responsible for the risks associated with the control system. Gless and Janal[56] address this issue by

stating rather obviously that, in principle, yes, but only if the error that has occurred stems from the producer's responsibility and organisational sphere. The problematic element in this statement, however, is precisely the content of the responsibility and organisational sphere of the various actors involved in the process of developing, producing, marketing, operating, programming, evaluating, and subsequently controlling autonomous systems. In this context, it will be relevant, for example, in terms of the timing of the occurrence of the error leading to the damage, to distinguish between those which existed at the time of delivery of the autonomous system and for which the producer is liable, and errors which occurred only as a result of updates to the system, the damage caused by which can be attributed to the entity within whose sphere of competence the software update falls (usually the producer, but it may be a completely different entity).

A significantly limiting factor when considering the standard of care regarding autonomous systems is their very nature, which is based on a process of self-learning, allowing them to make their own decisions as a result of the algorithms available and acquired through learning. These are influenced not only by the technical solutions directly from the producer but also by the information they have acquired from the external environment in the process of "learning". If these systems can learn certain behaviours and use them independently, they have the advantage that they do not need to be given strategies in advance to deal with specific problems, as not all potential issues can (and need to) be anticipated beforehand. However, this renders the system's behaviour somewhat unpredictable[57]. This can result in situations where a faulty algorithm or other error in the autonomous vehicle control software[58], incorrect assessment of the situation based on learned behavioural patterns can lead to damage, as well as situations where the damage occurred as a result of a decision by the autonomous system (hitting an oncoming vehicle to avoid a pedestrian who unexpectedly entered the roadway), but the control system did not exhibit any fault (on the contrary, it acted by the algorithm).

The question is how this impacts the standard of care itself, particularly with the producer. From an objective point of view, it is probably not reasonable to expect a reduction in the standard of care in such cases; on the contrary, it is a legitimate expectation that the producer should eliminate such erroneous decisions by the

system to the extent that this is possible and bearable[59]. The ability and capability of the entity to minimise or eliminate such risks is a critical factor in determining the objective standard of care. The risks of this process are known to the producers or other actors involved and can even be handled (it is possible to check what the system has learned first and then, after verification, include it in the decision-making process). Nevertheless, it is impossible to eliminate these risks, given the wide variety of situations that the system may encounter, the ongoing process of "learning", and the different learning experiences of various systems risks[60].

In summary, fault as a basis for the attribution of liability can be applied to establish responsibility for damage caused in relation to entities involved in the operation of autonomous systems, provided there is a demonstrable breach of the duty of care. This duty of care must be observed by the driver, producer, or any other relevant party connected to the autonomous system, regardless of or notwithstanding the system's uncontrollability[61]. This principle applies in cases where the harmful outcome could have been averted through appropriate care[62].

4.2. Attribution of liability based on grounds other than fault (liability of the operator, producer, and developer of autonomous public transport systems)

Given the limitations of fault-based liability as a basis for attribution in the context of autonomous public transport systems in smart cities, liability not based on fault will represent a significant element of tort law protection. The distinguishing feature of such liability is its connection to legally approved actions – namely, the creation of abstract risk – the realisation of which leads to a harmful outcome[63]. In such cases, risk is quantified based on the extent and likelihood of damage, typically involving risks arising from operating a transport vehicle, introducing such vehicles to the market, or implementing specific technologies[64].

Strict liability, not based on fault, is generally imposed when there is a significant imbalance between the ability to prevent damage and the injured party's capacity to avoid harm. In the context of public transport systems, the operator (e.g., transport companies or municipalities managing public transport within smart

cities) can be considered a liable entity based on the regulatory framework for damage caused by the operation of transport vehicles. In virtually all jurisdictions, this constitutes strict, no-fault liability.

It is already evident that the operation of autonomous vehicles in smart cities entails a degree of risk (though the precise scope of this risk cannot yet be determined) and a certain level of uncontrollability. This characteristic continues to justify strict liability due to the specific risks inherent in their operation[65].

Liability in such cases is assigned to the operator, defined as the entity with the legal and factual ability to control the given transport vehicle, where such control serves a longer-term functional purpose. This includes the entity on whose behalf, at whose risk, and in whose interest the vehicle is operated – typically, an entity that predominantly profits from the operation, has a vested interest in the system, and bears the financial costs of its operation[66].

Such attribution of liability to an entity that may not have actively contributed to the harm arises from the perception of the vehicle as a closed system characterised by specific operational risks for which the operator bears strict liability. The operator cannot, in their defence, claim that the autonomous system's behaviour was unpredictable or uncontrollable.

It is necessary to distinguish the operator as the person that carries out, implements, realises and has the legal and factual possibility to dispose of the given means of transport from the person that, due to the nature of the system requiring updates of the software component, assumes the legal and technical responsibility for the functional capability of the control system[67]. In most cases, this is the producer of the autonomous system, but this may not always be the case. The entity of the producer and the entity responsible for the functional capability of the control system may be different.

However, regarding fully autonomous control systems, it is unlikely that one will be able to clearly assess the situation since, in the case of a fully autonomous control system, the operator (city or transport undertaking) will have only minimal control over the system's behaviour. The resulting behaviour will be influenced by factors beyond the control of any legally recognised entity, whose contribution to the specific behaviour may vary and, consequently, be entirely debatable[68].

For this reason, considerations have also appeared in the literature questioning

the effectiveness of continuing to attribute damage to the system operator as the entity with the legal and factual ability to control the vehicle. In particular, considerations are directed towards a solution in which the liability of the autonomous system itself should replace the concept of attributability of damage to the operator[69]. The main reasoning behind this is the nature of the autonomous system as a "subject" endowed with intelligence, capable of reasoning and making decisions on its own based on the processing and evaluation of the information available to it, which would be granted subjectivity in the sense of the status of a form of "electronic person"[70]. However, as in the case of the liability of the controller, and given the nature of this "electronic person", it would be all the more necessary to link the liability of the autonomous system to some form of specific liability insurance at the same time as adopting such a solution. However, as the literature indicates, even in the case of autonomous driving systems, such a design is no more significant than the current liability of the operator of the means of transport, together with compulsory liability insurance.

Even if an autonomous system is found to be legally and illegally capable of wrongful conduct, transferring assets to that system would not make economic sense because such assets could only be used to cover the damage caused or provide insurance benefits. Moreover, such a competent scheme would have to be always represented by a natural person when it expresses its will (conclusion of the insurance contract, payment of premiums, payment of compensation, etc.)[71].

Moreover, imposing strict liability on a fully autonomous system operator does not always generate fair results. This is particularly the case if the means of transport falls outside the sphere of competence and control of the operator. Such a situation arises, for example, if another person takes over the means of transport without the knowledge or against the will of the operator.

In particular, this could involve various forms of unauthorised interference with the management system (e.g. hacking), which, given the nature of the system, cannot be completely ruled out. It is questionable whether such unauthorised interference with the management of an autonomous system can be attributed as a risk arising from the operation of public transport to its operator. We consider that such a fact does not fall within the scope of the risk in question and that it

would not be possible to hold the operator liable. On the contrary, it would be appropriate to impose strict liability on the unauthorised interferer in this case. However, this is a question of the setting of national legislation.

Developing and disseminating technology (*i.e.*, disseminating applicable knowledge as such) does not generally give rise to any liability aspects[72]. The mere development of a technology is unlikely to give rise to liability in itself, as such liability would be akin to liability for a scientific result. However, what could be considered for the future, in line with the risk-utility theory, is to impose liability on the developers if they would benefit economically from the system (which implies the use of the system) and if they would expose the public to the risk of the system[73]. In many cases, the developer is merged with the producer, who is already subject to liability for defects in products manufactured and placed on the market under Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

This almost forty-year-old regulation was not designed with a vision of the advent of autonomous technologies in mind and, therefore, shows significant limits in its application to damage caused by autonomous systems[74]. In December 2024, a new defective product directive came into force, which extends producer liability to defective software, including artificial intelligence systems. The challenges of the new directive, specifically those of autonomous driving systems, are discussed in the next section of the paper.

5. New horizons and upcoming trends in recent legislation to address the issues of liability for autonomous systems

Although in the previous section it was thoroughly drawn out that the liability for damage can be sufficiently addressed by existing scope of standard legislation (*i.e.* fault-based liability as well as strict liability), however some states have decided to cope with this challenging issue of specific liability by passing new regulations dealing with autonomous systems directly. Namely, Great Britain, Germany as well as Poland passed new laws or amended existing ones in order to particularly address these types of specific relations.

Great Britian passed a brand-new legislation called the Automated and Electric

Vehicles Act (the AEV Act)[75]. Apart from other parts of the AEV Act regarding mainly technical and administrative issues like charging and refuelling vehicles the Act deals in great amount of detail also with aspects of liability for damage. The Act divides strict liability not based on fault between insurer (Part 1, sec. 2(1) of the AEV Act) and owner of the vehicle (Part 1, sec. 2(2) of the AEV Act), however, it emphasizes insurers position regarding liability. Insurer of owner of the vehicle is liable for death or personal injury, or any damage to property with certain exclusions like damage to the vehicle itself, or to any carried goods or other property in custody of the insured person or the person in charge of the vehicle (Part 1, sec. 2(3) of the AEV Act). The Act also addresses an issue regarding negligence when it comes to unauthorised software alterations or negligence regarding proper installation of safety-critical software and its updates resulting with a possibility to exclude insurer's liability in these cases (Part 1, sec. 4 of the AEV Act).

The Act also states a contributory negligence of the harmed person if and when the accident was to any extent caused by the injured party (Part 1, sec. 3(1) of the AEV Act). Liability of insurer or owner of a vehicle for damage to the person in charge of the vehicle is fully excluded if the accident caused was wholly due to the person's negligence in allowing the vehicle to begin driving itself when it was not appropriate to do so (Part 1, sec. 3(2) of the AEV Act). However, it seems that the negligence on the part of the person in charge of the vehicle does not affect liability for other injuries or damage to property to harmed persons other than person in charge of the vehicle.

Germany on the other hand has chosen a different legislative approach. Although Germany did not pass a brand-new legislation, in 2017 the Road Traffic Act (Straßenverkehrsgesetz – StVG) was amended and automated vehicles were allowed to travel public roads. Although there were no specific provisions added to the liability regarding autonomous vehicles, an important element of the amended version of the StVG is an obligation to equip a vehicle with a system for data collecting on position and time when there is a change of entity controlling the vehicle from the system to the driver, when the system indicates to take control of the vehicle as well as when a technical fault occurs in the system (paragraph 63a StVG). Faulty failure of complying with obligations to take control of the vehicle when the need is signalised may establish a liability for

caused damage of a driver in charge of the vehicle.

In Poland, a definition of an autonomous vehicle was added through amendment of the Road Traffic Act (RTA) in order to define conditions and principles for conducting research works related to testing autonomous vehicles[76]. For the purpose of this testing a compulsory third party liability insurance of the research organizer is prescribed and one of many obligations of the organizer is to equip every autonomous vehicle by a driver ready to take control over the vehicle whenever needed to prevent any risk for causing damage to other parties[77].

It was already pointed out that the strict liability of the producer forms a possible ground for liability for the damage caused by autonomous vehicles. Regarding all the specifics regarding functioning of the autonomous vehicles described above, one of the crucial elements when it comes to risk of a caused damage is a software failure of the vehicle. Pursuant to previous Council Directive 85/374/EEC it was not clear whether software could be considered to be part of a "product" definition[78] for which a producer holds a rather strict liability. This shall be significantly changed pursuant to new Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective goods and repealing Council Directive 85/374/EEC (hereinafter as the new Product Liability Directive). The new Product Liability Directive is better suited for current technological and artificial-intelligence development. According to sec. 6 of the Preamble, no-fault liability for defective products should apply to all movables, including software, including when they are integrated into other movables or installed in immovables. This means that software regardless being installed in the autonomous vehicle, is considered to be a product pursuant to the new Product Liability Directive.

This means that regardless the integration, software alone is still considered to be a separate product from the vehicle itself. If a producer (a manufacturer) of a software is a different legal entity from the producer of the vehicle, strict product liability is still imposed on the software manufacturer. Unlike the previous directive, the new regulation provides a certain degree of protection to small subcontractors of software and related components to large motor vehicle manufacturers by excluding their liability in two cases. In the first case if the producer of the defective software component was, at the time of the placing on

the market of that software component, a microenterprise or a small enterprise (Article 3(2) of the Annex to Commission Recommendation 2003/361/EC) or the manufacturer in the product contractually agreed with the producer of the defective software to waive that right to claim damages.

Characteristic for the software as a product is that the manufacturer usually retains control over it even after placing it on the market and putting it into service in the form of system upgrades or updates by itself or via third party (Article 4 sec. 5(b)of the new Product Liability Directive). This aspect justifies continuous liability of the software producer up to the point of losing this control. This means that the manufacturer shall be held liable even for the defects of software occurring later through defective upgrades. If the software shall be substantially amended or modified either by software update or upgrade or due to the continuous learning of the system itself, the substantially modified product should be considered as available on the market or put into service at the time that modification is actually made. However, if a person using a vehicle or exercising control over it fails to upgrade the system and damage is caused due to lack of integrating the latest updates, producer is not liable due to contributory negligence if the owner of the vehicle itself is harmed or the causality link between defect of the product and damage is interrupted by another person's negligence. In these cases the owner of the vehicle or a person excercising control is liable based on fault.

In conclusion, the current approach to liability on both fault-based and not-fault-based principle seems to suffice the needs to regulate new horizons of liability relations when it comes to damages caused by autonomous vehicles. There are several options for an infringed party to claim damage and in practice it would not be rare that numerous obliged entities at once would be responsible at the same time. The standard approach is, whenever this happens, a formation of solidary obligation between all the responsible parties.

However, autonomous vehicles are specific when it comes to self-learning and self- or semi-self-sufficient driving system with little or no need of control by a present driver. With this regard the new German approach of obligation to equip a vehicle with a system for data collecting on position and time when there is a change of entity controlling the vehicle from the system to the driver seems to be a suitable way of ad a) dividing liability between either the driver or the

producer/the operator and ad b) building a system which significantly simplifies proving who and when was in charge of the vehicle and hence is responsible for the damage.
The current liability system is sufficient when it comes to damages caused by smart-city autonomous vehicles. However, due to possible imminent damage that may be caused on several lives at once or on property of quite a large scale, the importance of a suitable insurance system with clear limits for when and on what grounds the infringed parties may claim damage directly against the insurer of either the operator, the owner of the vehicle or the producer of the software might be a suitable way of risk allocation between all the affected parties. The more possible responsible entities, the more pressing is the issue of fair and equitable division of costs when it comes to plausible harm and injury.

6. Conclusion

Legal approach to resolving liability aspects of autonomous technologies is at least as important as the development and improvement of the technology itself. Despite the appearance that existing liability rules and concepts would be able to deal with the issue of liability for damage caused by autonomous control systems in their existing form and that there are already available means for the fair attribution of damage and distribution of risks associated with the operation and use of autonomous systems, this is not entirely true. The existing regulatory framework will not be totally able to cover the damage caused by the new generation of autonomous systems, which will be equipped with adaptive capabilities and the ability to learn by itself, which will inevitably be associated with a certain degree of unpredictability of behaviour. It is precisely for these aspects that it can be stated, taking into account the latest trends in newest regulation, whether at the national level of individual states or at the supranational level of EU regulation, that at the level of these specific relations, compulsory insurance is of a crucial importance, which suitably complements or even fully replaces the strict no-fault liability of operators, owners or producers of autonomous vehicles and their control components such as, mainly, software.

1. This article is a part of the implementation of the APVV project No. APVV-20-0171 "*Concurrence of delicts and quasi-delicts in non-contractual relations and their overlap with*

contract and property law".

2. Slogan "*Giving Cars the Power to See, Think, and Learn*" by NVIDIA, a Tesla partner in California.
3. See A. Taeihagh, H. S. M. Lim, *Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks*, in *Transport reviews*, 39, 2018, https://ssrn.com/abstract=3211839.
4. L. Collingwood, *Privacy implications and liability issues of autonomous vehicles*, in *Information and Communications Technology Law*, 1, 2017, pp. 32-45.
5. M. A. Richter, M. Hagenmaier, O. Bandte, V. Parida, J. Wincent, *Smart cities, urban mobility and autonomous vehicles: How different cities needs different sustainable investment strategies,* in *Technological Forecasting and Social Change*, 184, 2022, p. 1.
6. Last ride for RAC Intellibus as groundbreaking trial ends, (3rd of July 2023), available at https://southperth.wa.gov.au/about-us/news-and-publications/news-and-public-notices/news-detail/2023/07/03/last-ride-for-rac-intellibus-as-trial-ends.
7. T. Andrejčák, *Mercedes-Benz Future Bus: This bus rides alone. And it's perfect at it*, 20th of November 2017, https://auto.pravda.sk/magazin/clanok/448138-mercedes-benz-future-bus-tento-autobus-jazdi-sam-a-ide-mu-to-skvelo/
8. J. Procházka, *In China they have a hybrid - a train and a bus in one. It runs on drawn tracks*, 7th of June 2017, https://www.techbox.sk/v-cine-maju-hybrid-vlak-autobus-v-jednom-jazdi-po-nakreslenych-kolajach.
9. M. Biel, *Germany tests first self-driving tram. A stroller gets in its way*, 27th of September 2018, https://www.trend.sk/technologie/nemecku-otestovali-prvu-samojazdiacu-elektricku-cesty-jej-vtlacili-kocik.
10. R. Mališka, *The world's first autonomous tram runs in Germany,* 25th of September 2018, https://techpedia.ta3.com/veda-a-vyvoj/novinky/5923/v-nemecku-jazdila-prva-autonomna-elektricka-na-svete.
11. P. Steigauf, *Radical change in public transport: The end of bus drivers? Robo-buses will soon flood cities*, 27th of November 2024, https://www.proficars.sk/novinky/radikalna-zmena-mhd-koniec-soferov-autobusov-robo-busy-vraj-coskoro-zaplavia-mesta/1577.
12. *Autonomous buses in public transport, what's going on? An overview of projects, technology, challenges*, 19th of December 2024, https://www.sustainable-bus.com/its/autonomous-bus-public-transport-driverless/.
13. N. Lavars, *Volvo's first electric driverless bus swings into action in Singapore*, 6th of March 2019, https://newatlas.com/volvo-first-electric-driverless-bus-singapore/58743/.
14. *Volvo 7900 Electric*, 25th of October 2019, https://landtransportguru.net/volvo-7900-electric/.
15. *Autonomous buses in public transport, what's going on? An overview of projects, technology,*

challenges, 19th of December 2024, https://www.sustainable-bus.com/its/autonomous-bus-public-transport-driverless/.

16. R. Mališka, *The world's first autonomous tram runs in Germany*, 25th of September 2018, https://techpedia.ta3.com/veda-a-vyvoj/novinky/5923/v-nemecku-jazdila-prva-autonomna-elektricka-na-svete.
17. *CAVforth Bus wins first Self-driving Industry Vehicle of the Year award,* 23rd of November 2023, https://www.smmt.co.uk/2023/11/cavforth-bus-wins-first-self-driving-industry-vehicle-of-the-year-award/.
18. L. Dyson, *The world's largest-capacity autonomous bus service*, 2nd of November 2023, https://pagely.traffictechnologytoday.com/news/autonomous-vehicles/feature-the-worlds-largest-passenger-capacity-autonomous-bus-service.html.
19. *Plan of autonomous mobility up to 2025 of the Ministry of Transporation of the Czech Republic dated 10th April of 2024*, https://md.gov.cz/getattachment/Uzitecne-odkazy/Autonomni-mobilita/asdasd/CZ_Plan_Autonomni_mobility.pdf.aspx.
20. *Karsan's e-Atak Autonomous, green light to enter regular traffic in Norway,* 1st of March 2024, https://www.sustainable-bus.com/news/karsans-e-atak-autonomous-green-light-to-enter-regular-traffic-in-norway/.
21. L. Čížová, *The city tested the technology for autonomous public transport control*, 30th of April, 2021, http://inba.sk/vismo/dokumenty2.asp?id_org=600185&id=4842&p1=8825.
22. *Sophisticated public transport management will help reduce emissions*, 27th of April 2021, https://smartmobility.gov.sk/sofistikovane-riadenie-mhd-pomoze-znizovat-emisie/.
23. *Platform of cooperation ‚Intelligent Mobility of Slovakia'*, 27th of April 2021, https://smartmobility.gov.sk/o-nas/platforma-spoluprace-inteligentnej-mobility-slovenska/.
24. P. Steigauf, *Radical change in public transport: The end of bus drivers? Robo-buses will soon flood cities*, 27th of November 2024, https://www.proficars.sk/novinky/radikalna-zmena-mhd-koniec-soferov-autobusov-robo-busy-vraj-coskoro-zaplavia-mesta/1577.
25. S. Zhang*, HK's largest autonomous bus transportation system to launch next year*, 4th of July 2024, https://www.chinadailyhk.com/hk/article/587275.
26. G. Hornung, *Rechtsfragen der Industrie 4.0. Datenhoheit - Verantwortlichkeit - rechtliche Grenzen der Vernetzung,* Nomos, Baden-Baden, 2018, p. 30.
27. For algorithmic decision-making systems see K. A. Zweig, T. D. Krafft, *Fairness und Qualität algorithmischer Entscheidungen*, in R. Mohabbat Kar, B. E. P. Thapa, P. Parycek (eds.), *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft,* Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Kompetenzzentrum Öffentliche IT (ÖFIT), Berlin, 2018, pp. 204-227.

28. For more on causality see C. Müller-Hengstenberg, S. Kirn, *Kausalität und Verantwortung für Schäden, die durch autonome smarte Systeme verursacht werden. Eine Untersuchung der deliktischen Haftung für den Einsatz autonomer Software-agenten*, in *Computer und Recht*, 10, 2018.
29. Compare H. Zech, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in S. Gless, K. Seelmann (eds.), *Intelligente Agenten und das Recht,* Nomos Verlagsgesellschaft, Baden-Baden, 2016, p. 164.
30. On the criminal aspects, see e.g. S. Beck, *Selbstfahrende Kraftfahrzeuge – aktuelle Probleme der (strafrechtlichen) Fahrlässigkeitshaftung*, in B. H. Oppermann, J. Stender-Vorwachs, *Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen,* C. H. Beck, München, 2017, pp. 33-59.
31. G. Spindler, *Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?,* in *Computer und Recht*, 12, 2015, p. 766; also S. Horner, M. Kaulartz, *Haftung 4.0. Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme,* in *Computer und Recht*, 1, 2016, p. 7.
32. M. R. Calo, *Open Robotics*, in *Maryland Law Review*, 3, 2011, p. 125.
33. G. A. Bekey, *Autonomous Robots: From Biological Inspiration to Implementation and Control*, Massachusetts Institute of Technology, Massachusetts, 2005, cit. by H. Zech, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in S. Gless, K. Seelmann (eds.), *Intelligente Agenten und das Rec,* Nomos Verlagsgesellschaft, Baden-Baden, 2016, p. 168.
34. Compare H. Zech, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in S. Gless, K. Seelmann (eds.), *Intelligente Agenten und das Rec,.* Nomos Verlagsgesellschaft, Baden-Baden, 2016, p. 168.
35. *Ibid*., p. 169.
36. *Ibid*., p. 176.
37. See also T. M. Gasser, *Grundlegende und spezielle Rechsfragen für autonome Fahrzeuge*, in M. Maurer, J. CH. Gerdes, B. Lenz, H. Winner, (eds.), *Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte,* Springer, Berlin, 2015, p. 552.
38. A study by The National Highway Traffic Safety Administration (NHTSA) revealed that 94% of traffic crashes are due to human factors (National Highway Traffic Safety Administration Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety 5, 2016, www.transportation.gov/AV), and it is autonomous vehicles (while obviously unable to eliminate all of these crashes) that can make a significant contribution to improving road safety, with expert studies reporting reductions in vehicle collisions of up to 80% (J. Albright et al., *Automobile insurance in the era of autonomous vehicles. Survey results*, 2015, https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/kpmg-automobile-insurance-in-era-autonomous.pdf). This is an estimate that foresees a massive replacement of the current 0-2, highly automated and fully automated driving stages with 3-5 driving stages. However, due to the gradual introduction of autonomous-driven vehicles, the above

percentage reduction in accidents will not be a blip; studies indicate that by 2035 it should be in the range of 7-15%. These are figures that refer to individual means of transport.

39. A. Goldman, *Bubble? What bubble?*, in *The New York Times Magazine*, 7th of July, 2011, https://www.nytimes.com/2011/07/10/magazine/marc-andreessen-on-the-dot-com-bubble.html.
40. For more on risk as a criterion for allocating damages, see S. Meder, *Risiko als Kriterium der Schadensverteilung*, in *Juristenzeitung*, 11, 1993.
41. See T. M. Gasser, *Grundlegende und spezielle Rechsfragen für autonome Fahrzeug,* in M. Maurer, J. CH. Gerdes, B. Lenz, H. Winner, (eds.), *Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte,* Springer, Berlin, 2015; S. Gless, R. Janal, *Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung*, in *Juristische Rundschau*, 10, 2016; S. Horner, M. Kaulartz, *Haftung 4.0. Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme,* in *Computer und Recht*, 1, 2016; H. Zech, *Gefährdungshaftung und neue Technologien*, in JuristenZeitung, 1, 2013.
42. According to this theory, risks should be objectively attributed to whoever is able to control and manage them, given the fact that the risk originates in his or her sphere of competence, H. B. Schäfer, C. Ott, *Lehrbuch der ökonomischen Analyse des Zivilrechts*, 1 Aufl., Springer Berlin, Heidelberg, New York, 1986, p. 152. Usually, the person who is allowed to control and operate the system in certain circumstances is the user, operator or producer of the system in question. If a certain probability of damage is "attributable" predominantly to one party, it thus seems fair to attribute to that party the damage that has been realised within that probability, J. Esser, H. L. Weyers, *Schuldrech*t, Band II, Besonderer Teil, 7 Aufl., C. F. Müller Juristischer Verlag, Heidelberg, 1991, p. 537.
43. Following the theory of increased risk, responsibility is imposed on those who have created such increased risk through their operations to motivate them to take the utmost care of all aspects of the systems' operation and implement the necessary control and protection measures. In relation to autonomous control systems in general, it is the producer or operator who, given his position as a management, organisational and control mechanism, is best placed to deal with the hazards arising from the operation of the autonomous control system. It therefore seems fair to attribute to it those risks which originate in its sphere, from which it benefits and which it can control most effectively.
44. R. Polčák, *Liability of Artificial Intelligence and Information Formations without Legal Personality*, in *Bulletin of Advocacy*, 11, 2018, p. 24.
45. In this case, it is primarily a question of proving causality between the cause of the damage itself and the adverse consequence or the explicit or analogous subsumption of the functioning of autonomous systems under the already existing liability concepts of tort law. In relation to the definition of causation, factual causation itself is problematic, defined in tort law in terms of the causal rules of the *conditio sine qua non* formula in the continental system of law or the but-for test in the Anglo-American system of law. As Polcak argues, it is never possible to retroactively reconstruct the robot's operating code

and determine why the robot did or did not do something any more than it is logically possible to determine what factors were involved in the robot's operating code, *i.e.*, why, in effect, the robot programmed itself in a certain way, R. Polčák, *Liability of Artificial Intelligence and Information Formations without Legal Personality*, in *Bulletin of Advocacy*, 11, 2018, p. 24. For this reason, it is questionable whether, with this unclear chain of causation, an imputable link can be defined in the sense of the theory of adequate causation (C. Müller-Hengstenberg, S. Kirn, *Kausalität und Verantwortung für Schäden, die durch autonome smarte Systeme verursacht werden. Eine Untersuchung der deliktischen Haftung für den Einsatz autonomer Software-agenten*, in *Computer und Recht*, 10, 2018, p. 686) or on what basis the criteria and conditions of legal causation can be established in this relationship of unclear factual causation.

46. S. Grundmann, *§ 276 R. 50,.* in *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB,* 7. Aufl.*,* C. H. Beck, München, 2016.
47. Cf. M. Novotná, M. Jurčová, *Liability for damage caused by autonomous and semi-autonomous vehicles under Slovak law,* ŠafárikPress UPJŠ, Košice, 2018.
48. For example, at vehicle autonomy level 3, the autonomous system is able to control the steering while monitoring the environment in which it is moving, but the driver is required to be able to respond appropriately to the system's request to intervene in the control of the vehicle.
49. T. M. Gasser (ed.) *Rechtsfolgen zumehmender Fahrzeugautomatisierung*, Berichte der Bundesanstalt für Straβenwesen, Fahrzeugtechnik, Heft F 83, Verlag für neue Wissenschaf, Bremerhaven, 2012, p. 13 ff.
50. Also S. Horner, M. Kaulartz, *Haftung 4.0. Verschiebung des Sorgfaltsmaβstabs bei Herstellung und Nutzung autonomer Systeme,* in *Computer und Recht*, 1, 2016, p. 9.
51. *Ibid*.
52. Novotná, M., Jurčová, *Liability for damage caused by autonomous and semi-autonomous vehicles under Slovak law,* ŠafárikPress UPJŠ, Košice, 2018.
53. Problematic in this context is not only the fact that there are no specific normatively captured technical standards and requirements for autonomous control systems, but also the fact that due to the speed of development of the IT sector, such standards may become rapidly outdated.
54. It is clear that the obligation to maintain standards of science and technology affects those that have been tested in practice as the most effective and have therefore been generally accepted.
55. In 2015, a pair of hackers hacked into the systems of a Jeep Cherokee in a controlled experiment (which was conducted in normal traffic) by remotely hacking a connected vehicle. The "attackers" were able to remotely control the air conditioning and other cabin features, disable the automatic transmission, and disable the brakes. They could even take control of the vehicle if reverse gear was engaged. For more, see A. Greenberg, *Hackers remotely kill a jeep on the highway - with me in it*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

56. S. Gless, R. Janal, *Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung*, in *Juristische Rundschau*, 10, 2016, p. 568.
57. G. Hornung, *Rechtsfragen der Industrie 4.0. Datenhoheit - Verantwortlichkeit - rechtliche Grenzen der Vernetzung,* Nomos, Baden-Baden, 2018, p. 31.
58. In March 2018, a tragic incident occurred in the state of Arizona when a pedestrian died because of a collision with an autonomously driven Uber vehicle (this was the first recorded case of a human being killed by being struck by a robot-driven vehicle in a normal operation). In May 2018, Uber issued a statement saying that the probable cause of the autonomous vehicle prototype collision was a problem in the software, which is tasked with deciding how the vehicle should react to objects it detects. While the vehicle's sensors detected the presence of a pedestrian crossing the road with a bicycle, the software decided that the vehicle did not need to respond immediately. That decision resulted from an algorithm that requires Uber's software, like that of other autonomous systems, to ignore false positives or objects in the vehicle's path but not a problem for the vehicle (e.g., a plastic bag in the air), A. Efrati, *Uber Finds Deadly Accident Likely Caused By Software Set to Ignore Objects On Road*, https://www.theinformation.com/articles/uber-finds-deadly-accident-likely-caused-by-software-set-to-ignore-objects-on-road?shared=56c9f0114b0bb781.
59. T. Hey, *Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Strassenverkehr,* Springer, Gabler, Wiesbaden, 2019, p. 63.
60. S. Kirn, C. D. Müller-Hengstenberg, *Rechtliche Risiken autonomer und vernetzter Systeme*, De Gruyter, Oldenbourg, 2016, p. 102 ff.
61. The mere fact that the autonomous system as a whole or some of its components are not generally considered controllable never does and cannot lead to the exemption of the entity concerned (usually the producer in this context) from the obligation to compensate for the damage caused. On the contrary, it leads to a higher standard of care regarding the safety obligations of development, production and subsequent control.
62. S. Horner, M. Kaulartz, *Haftung 4.0. Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme,* in *Computer und Recht*, 1, 2016, p. 8.
63. H. Zech, *Gefährdungshaftung und neue Technologien*, in *JuristenZeitung*, 1, 2013, p. 21.
64. *Ibid*., p. 22.
65. M. Novotná, *Liability for damage caused by the operation of means of transport*, in M. Števček, et al., Civil Code. Commentary, C. H. Beck, Prague, 2015.
66. *Ibid.*
67. For a more detailed definition of this person, see S. Gless, R. Janal, *Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung*, in *Juristische Rundschau*, 10, 2016, p. 562.
68. U. Bose, *The black box solution to autonomous liability*, in *Washington University Law Review*, 5, 2015, p. 1325.
69. See e.g. considerations of H. Zech, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in S. Gless, K. Seelmann (eds.),

Intelligente Agenten und das Recht, Nomos Verlagsgesellschaft, Baden-Baden, 2016, p. 179.

70. On the status and analysis of the conditions for granting legal personality to artificial intelligence, see J. Zibner, *Acceptance of legal personality in the case of artificial intelligence,* in *Review of Law and Technology*, 17, 2018; S. M. Solaiman, *Legal personhood of robots, corporations, idols and chimpanzees: a quest for legitimacy*, in *Artificial Intelligence and Law*, 2, 2017, pp. 155-179.
71. S. Gless, R. Janal, *Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung*, in *Juristische Rundschau*, 10, 2016, p. 571.
72. H. Zech, *Gefährdungshaftung und neue Technologien*, in *JuristenZeitung*, 1, 2013, p. 28.
73. *Ibid*.
74. The limits result in particular from the nature of the Directive as a pro-consumer regulation, conferring standing only on a victim who has suffered injury to life or limb or damage to an object other than the defective product itself, which object must normally be intended for personal use or personal consumption and predominantly serve that purpose for the victim. It follows that the enhanced producer liability under the Product Liability Directive should not apply to damage caused by autonomous systems used on public goods, municipal property, systems not used for personal use (the above means that autonomous transport in smart cities is not covered by the Directive).
75. https://www.legislation.gov.uk/ukpga/2018/18/pdfs/ukpga_20180018_en.pdf.
76. E. Jędrzejewska, *Autonomous vehicles and the issue of liability for damage caused by the movement of such vehicle*, In *Journal of Modern Science*, 2, 2023, Vol. 51, p. 635.
77. *Ibid*. p. 636.
78. Ľ. Sisák, *Artificial intelligence and the Slovak law of obligations: non-conforming performance and non-contractual liability arising out of damage caused to another*, in J. Klučka, L. Bakošová, Ľ. Sisák (eds.), *Artificial intelligence from the perspective of law and ethics: contemporary issues, perspectives and challenges*, Praha, Leges, 2021, pp. 156-157.

Privacy in Smart Cities

Richard Pomahač

DOI: 10.13130/2723-9195/2025-2-14

Gli sviluppi tecnologici e i rischi di minacce informatiche stanno portando a un cambiamento nella percezione della privacy nelle smart city. Il concetto di città intelligenti si basa sulla raccolta continua e onnipresente di dati. Negli ultimi anni si è acceso un dibattito sul fatto che la società si stia muovendo verso l'azzeramento della privacy nell'era digitale. È emerso il termine privacy digitale, che risponde alla preoccupazione che tutto ciò che non appartiene al pubblico ma è impegnato in forma digitale possa essere soggetto a una distribuzione immediata e inevitabile. La progettazione di Humane Smart Cities riflette la necessità che il potere della tecnologia si manifesti in connessione con gli interessi autentici degli abitanti della città. Più recentemente, incontriamo il progetto Smart Cities More Than Human, che crea uno spazio ibrido socialmente ed ecologicamente equo. Tuttavia, ciò non cambia il fatto che viviamo in un'epoca in cui le persone non possono semplicemente ritirarsi nella privacy rifiutando di usare certe tecnologie. Le tutele per la privacy consentono alle persone di utilizzare i servizi delle smart city senza temere inutili interruzioni o distorsioni.

Technological developments and the risks of cyber threats are prompting a change in the perception of privacy in smart cities. The concept of smart cities relies on continuous, ubiquitous data collection. In recent years, there has been a heated debate about whether society is moving towards zero privacy in the digital age. The term digital privacy has emerged, addressing concerns that anything that does not belong to the public but is committed to digital form may be subject to immediate and inevitable distribution. The design of Humane Smart Cities reflects the need for the power of technology to manifest itself in connection with the authentic interests of the city's inhabitants. Most recently, we encounter the Smart Cities More Than Human project, creating a socially and ecologically fair hybrid space. However, this does not change the fact that we live in an age where people cannot simply withdraw into privacy by refusing to use certain technology. Privacy safeguards allow people to use smart city services without fear of unnecessary disruption or distortion.

Summary: 1. Introduction.- 2. Smart cities paradigm.- 3. Privacy as a legal concept.- 4. Informational privacy.- 5. Conclusions.

1. Introduction

Considerations about privacy in smart cities are foreshadowed by a sentence found in the well-known book The Death and Life of Great American Cities, first published in 1961. In this book, Jane Jacobs emphasises several times that good city planning must aim for at least an illusion of isolation and privacy[1]. «*Privacy is precious in cities. It is indispensable. Perhaps it is precious and indispensable everywhere, but in most places, you cannot get it*»[2].

In the 1960s, the concept of a smart city, which provides technological answers to the challenges and improvements in the quality of life for most of the world's population living in urban centres and conurbations, was not yet in existence. However, the notion that privacy provides individuals and groups in society with the ability to maintain autonomy and secure communication was already well-founded.

Jane Jacobs did not explicitly address the rise of modern technology in her later works. However, her conviction that elementary values are being underestimated, which should be seen as a civilisational problem, remained unchanged even in times when the slogan "smart solutions" had become ubiquitous. In her last book, Dark Age Ahead from 2004, she warned against mindless progressive thinking and the arrogance that comes with it. «*Ironically, societies (including our own) that have been great cultural winners in the past are in a peculiar situation of failing to adapt successfully in the face of new realities. This is because nothing succeeds like success, and it follows that nothing hangs on past its prime like past success*»[3].

How do modern technologies affect urbanisation? And how can the law that guarantees respect for privacy help with this? We will address these questions in the following explanation.

2. Smart cities paradigm

From the 1960s, approaches associated with the automatic generation and processing of large data sets gradually began to gain ground in urban planning theory and practice. As Mark Vallianatos reminds us, the concept of smart cities seems like a contemporary urbanism trend. Still, cities have been using technology to gather, interpret, and visualise civic data for many decades. «*Like many smart, new ideas, however, it's not new. Is not even new to Los Angeles, which has been pursuing computer-assisted data and policy analysis for decades. Beginning in the late 1960s and through most of the 1970s, the little-known Community Analysis Bureau used computer databases, cluster analysis, and infrared aerial photography to gather data, produce reports on neighbourhood demographics and housing quality, and help direct resources to ward off blight and tackle poverty*»[4]. Even after half a century, the volumes of "The State of the City Reports" convince us that Los Angeles deserves to be called "The Know-How City"[5]. Data unlocked know-how. Los Angeles could be proud of the sophisticated planning that would improve the infrastructure on which the city depends.

If we read urban planning considerations from half a century ago, we still do not come across the label smart city in them. At that time, the attribute smart was reserved for people rather than things or technologies. After all, it was not until the end of the 1980s that the phrase "ubiquitous computing" appeared, followed by the concept of the Internet of Things. It was becoming a convenience of technology that even things began to behave as if they were being controlled by intelligence. That was probably the reason why cities were starting to get brilliant from a theoretical perspective.

Islands of intelligent enclaves have long been seen as technopoles. Technopole describes space dedicated to technological innovation. Technologies change habits of thinking. As Marina Christodoulou concludes, «*For a new tool, medium, technique, or technology to flourish or to be used as such, the milieu of the culture and the worldview or the thinking environment has to change in order to be fit and welcoming for its use, or even render the tool as necessary*»[6]. Although growth has been the dominant ideology in most locales in the United States, there has always been a subversive thread of resistance challenging the

technopoles as a society in which lives, thoughts, and happiness are regulated by technology[7].

Thinking about the future of cities has become fertile ground for technological optimism for many authors. This vision envisioned a wired city with advanced complexes connected by satellites and fibre optics. Networked cities were populated by "knowledge processors" engaged in the rapid exchange of information. By adapting quickly and flexibly to global markets, digital towns have become more efficient and competitive[8].

In the surviving atmosphere of this approach, a conference was held in San Francisco in 1990 called The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks. The use of the term smart city was rather daring at the time, and the organisers of this conference had no ambition to create a new slogan or metaphor. Global networks attracted the most attention from the participants. Adequate attention was paid to technological breakthroughs and human resources with the aim of accelerating the development of high-tech, in short, fast systems. Regarding the urban planning topic, it can be said that the conference was dedicated to smart infrastructure rather than smart cities. Michael Wakelin put it nicely. «*Infrastructure must be made global, fast, and smart*»[9].

The discussion of the technopole phenomenon in the early 1990s pointed to a two-fold point of view. On the one hand, the city was explored in terms of social integration and sense of space. On the other side, there has been the question of economic growth and new services supported by political initiatives that aim to make a difference. There was consensus that both approaches must consider globalisation trends. However, it became clear that the already established technopole concept pursues conflicting goals than the smart infrastructure concept. Technopolis is all about innovations. Smart infrastructure combines the most advanced available technologies with traditional infrastructure to create wired, efficient, and sustainable cities. In this sense, virtual city infrastructure is about efficiency and sustainability.

As Alessandro Aurigi and Stephen Graham reported back in the 1990s, governments responded to the urban crisis by creating hundreds of experimental high-tech virtual cities. This was due to the extraordinary user-friendliness of the web interface and the ability of the website itself to allow access from virtually

anywhere. Such cities either use a familiar interface as a metaphor to group a wide range of Internet services located around the world, or they have a positive feedback loop related to the development of specific cities. They can, therefore, be perceived either as an advertising and promotional area or as a digital space supporting political and social discourses about the city itself[10].

Experts who placed great emphasis on the global dimension of the innovative infrastructure problem were not wrong. This was demonstrated at the turn of the millennium when intelligent enclaves began to network on a worldwide scale. But previously hidden issues have also emerged. Arun Mahizhnan aptly expressed them in 1999 in connection with the implementation of a massive smart infrastructure program in Singapore. «*The challenge of converting the ignorant or sceptical onlookers to the new technologies is already a major challenge. But an even greater challenge is to put IT in the service of humankind instead of using it for the subversion or the destruction of the values and ways of life people hold dear*»[11].

At the turn of the millennium, the topic of smart cities boomed. As found by L. Mora, R. Bolici and M. Deakin, with the assistance of the scholarly engine developed by Google, between 1992 and 2015, there were 25,770 publications on this topic produced: the annual production of publications on smart cities increased by 600 times within 24 years, moving from 16 in 1992 to 9,494 in 2015[12]. Professional literature has responded to the fact that in the first decade of the 21st century, for various reasons, cities all over the world began to declare themselves smart, and that is why the scope of this transformation was also initially very different.

When the trademark "Smarter City" was officially registered for the international technology company IBM in November 2011, it seemed that the concepts could quickly be clarified[13]. Cities should be more innovative if they are instrumented, connected, and intelligent. This meant the ability to 1. capture live real-world data, 2. integrate that data into a computing platform, and 3. leverage data processing, visualisation services, and artificial intelligence for better operational decision-making. But can innovative technologies change governance? M. Foucault said in one conversation: «*I must say that what interests me more is to focus on what the Greeks called the techne, that is to say, a practical rationality governed by a conscious goal. I am not even sure if it is worth constantly asking the question of whether the government can be the object of an exact science... The*

disadvantage of this word techne, I realise, is its relation to the word technology, which has a particular meaning»[14]. The philosophical question of whether technologies based on the rationality (but also the irrationality) of automated data processing and artificial intelligence will make cities better is highly relevant. Recently, Daniele Marongiu returned to the Foucauldian theme and recalled that a smart city does not necessarily mean technological innovation but rather the innovation of concepts and ideas. His thoughts end with the sentence: «*For this reason, the most iconic symbol of smart cities is probably not a smartphone, but the boarding area of a busy airport with a grand piano at its centre*»[15].

3. Privacy as a legal concept

Human privacy is a comprehensive and, in many ways, elusive concept. In the past of humanity, privacy was often reduced to such an extent that even the most intimate area, from today's perspective, was not included. In the 1990s, the debate about whether society in the digital age is returning to zero privacy has rekindled. A key question raised was whether, in the digital age, individuals would maintain, lose, or gain control over information about themselves[16]. The term digital privacy appears, facing fears that soon, anything not belonging to the public but committed to a digital form may be subject to immediate and inevitable distribution. Will Thomas DeVries directly stated in this context that there is a consensus among privacy scholars that privacy law and theory must change to meet the needs of the digital age[17].

The tendency to protect privacy has manifested itself in various forms for a very long time. Bernardo Periñán recalls that privacy, like freedom, is a natural feeling of every human being. Otherwise, we would live in a prehistoric collectivism in which individuals have lost their self-awareness. «*Like the roots of the concept of citizen, to which privacy is very closely related, the origin of this legal construction lies in ancient Rome... In sum, it could be said that the problem of privacy is related to the problem of freedom and the recognition of personal individuality by a political system because only on that basis can privacy be considered a legal value... The person as a holder of a true right to privacy must have the choice to allow others into this personal ambit*»[18]. While classical Roman law made it possible to defend the right to privacy against non-public intruders in civil court,

subsequent legal developments were not straightforward. As Mia Korpiola concludes, the dividing line between public and private space was porous and situational in the medieval and early modern periods. Privacy as a right is neither a medieval nor an early modern phenomenon. Indeed, the right to privacy presupposes advanced legal protection of the individual, suggesting that it could only develop when pre-modern collective value systems and worldviews began to disintegrate slowly[19].

John Locke's words inspired the concept of privacy: «*Every man has a property in his person: this nobody has any right to but himself*»[20]. Locke thus expressed the inalienable right of the human person and connected the right to oneself with the theme of property. Subsequently, many legal disputes took place within this framework of reasoning, which aimed to reveal the nature of privacy and inviolable rights.

This illustrates well the approach to the argument that literary publication is no longer an exclusive private right. In 1769, the Court of King's Bench provided that an author enjoyed the exclusive right to publish his work in perpetuity. Mr Justice Yates took the minority view that the perpetual right could not be upheld because, in the case in question, the author, having already exercised the option of publication, had forfeited the exclusive right. «*Most certainly, the sole proprietor of any copy may determine whether he will print it or not... Ideas are free. However, while the author confines them to his study, they are like birds in a cage... It is certain every man certainly has a right to keep his sentiments if he pleases: he has certainly a right to judge whether he will make them public or commit them only to the sight of his friends. In that state, the manuscript is, in every sense, his peculiar property, and no man can take it from him or make any use of it which he has not authorised without being guilty of a violation of his property. And as every author or proprietor of a manuscript has a right to determine whether he will publish it or not, he has a right to the first publication, and whoever deprives him of that priority is guilty of a manifest wrong; and the Court have a right to stop it. But this does not apply to the present question: this author published it many years ago and received a profit from it*»[21].

Modern constitutionalism responded to the potential threat to privacy from public authorities and the expanding media industry already at a time when the positive definition of privacy was still in its infancy. Rather than the right to

privacy, the right to be secure was constructed with a more sensitive relationship to threats to safety and seclusion.

Let's see how this is expressed, for example, in the U.S. Bill of Rights: «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated*». This text does not explicitly mention the right to privacy, but it has contributed significantly to the definition of privacy in terms of personal and property freedom and security. Legal thinking about privacy was more intensively in touch with the different concepts of the inviolability of persons and property and with the ever-improving possibilities of making visible and expanding what was previously hidden. Moreover, regarding the right to be secure, invasions of privacy using modern technology, such as the internet and drones, which no one had a clear idea about in the 19th century, are assessed[22].

With the emergence of an industrialised and mass society, there have been several attempts to shed the burden of tradition and create a compelling and easy-to-remember legal concept of privacy. In 1879, Thomas M. Cooley included in his classification of rights and duties the right to oneself, which corresponds to the duty to avoid harmful contact with other persons. «*The right to one's person may be said to be a right of complete immunity: to be let alone*»[23].

This peculiarity might have faded away if it had not been resurrected by Samuel D. Warren and Louis D. Brandeis in a famous article that reacted, among other things, to the unacceptable practices of the mass media. In 1890, there was not yet talk about dangerous social networks and surveillance practices in smart cities, but about the fact that instantaneous photographs have invaded the sacred precincts of private and domestic life and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops[24].

Suppose we proceed from the findings of W. L. Prosser. In that case, the protection afforded by American courts has evolved so that the right to privacy has slowly but surely come to be recognised as immediately effective. Case law has established types of tortious conduct, in particular, invasion of privacy or private affairs, public disclosure of embarrassing private facts, or publicity that puts a person in a false light before the public[25].

The belief that privacy is what allows human beings "to be who they are" is

reflected in the Universal Declaration of Human Rights, whose Article 12 affirms that no one shall be subjected to arbitrary interference with his privacy. This formulation demonstrates developments in legislation and case law in many countries and, to some extent, completes the path to the right to privacy in the sense of being let alone. The Declaration was proclaimed at the end of 1948 when a new phase of the information age was beginning. From the mid-20th century to the 1980s, television, computers and satellites connected the world and prepared society for the use of today's digital technologies[26].

As Stewart Brand wrote, the real legacy of the 1960s generation is the computer revolution. This generation «*proved in cyberspace that where self-reliance leads, resilience follows, and where generosity leads, prosperity follows. If that dynamic continues, and everything so far suggests that it will, then the information age will bear the distinctive mark of the countercultural '60s well into the new millennium*»[27]. The cultural shift that Brand wrote about affected the concept of privacy as well. Right to be left alone was no longer on the agenda. Fred Turner believes this was a justification for a return to the mainstream world, citing Brand's 1975 reflection: «*Self-sufficiency is an idea which has done more harm than good (...). It is a charming woodsy extension of the fatal American mania for privacy (...). It is a damned lie. There is no dissectable self. Ever since there were two organisms, life has been a matter of co-evolution, life growing ever more richly on life (...). We can ask what kinds of dependency we prefer, but that's our only choice*»[28].

But what would be the point of the choice? What kinds of dependency do we prefer? Let's focus on an aspect directly related to the topic of smart cities. Technological progress made it possible about half a century ago for automated data systems to acquire an irreplaceable role, even at the level of individual residential communities. As A. Downs explained at the time, the technical design of these systems seemed exciting and more amenable to analysis because computer companies naturally focused on describing the impressive improvements they could provide. Doubts were thus dispelled that better information would reduce the frequency and extent of planning and decision-making errors[29]. There is no doubt that since the 1960s, the technical possibilities to obtain data have improved significantly. In this respect, it is, therefore, indifferent to what personal preferences for dependency are. That is

why privacy is mortal. Bogdan Hoanca reminds us in this context that the most insidious aspect of the death of privacy is that privacy is no longer an individual choice. «*Some people love the small village life, and some people hate it, but as privacy continues to be eroded and may even disappear, humankind will end up living in the virtual equivalent of a "small" village – where everybody knows or can know everything about everybody else – and where the village comprises the entire world*»[30].

The embarrassment over the mortality of privacy was successfully overcome in the book Privacy and Freedom. A. F. Westin softened the emphasis placed on the right to be let alone, as the individual's clinging to solitude and self-sufficiency is never absolute, as participation in society is an equally strong desire. He also did not underestimate the dangers of the digital age and developed a new concept of the right to privacy. «*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*»[31]. Westin's work has led to considerations about the protection of personal data as an integral part of the right to privacy.

4. Informational privacy

The International Covenant on Civil and Political Rights, which was adopted at the end of 1966 and entered into force in March 1976, established in Article 17 that no one shall be subjected to arbitrary or unlawful interference with his privacy.

The word unlawful has been added compared to the relevant provision of the Universal Declaration of Human Rights. An extensive comparative study prepared for the Nordic Conference on privacy in 1967 makes clear the shift in meaning that took place at that time. The study recalled that it is not only in police states that public authorities can encroach more effectively than ever on the sanctity of the private sphere. The space for the regulation of private life was prepared not only by the concentration and expansion of the executive power but also by accepting the idea of the supremacy of the community, considered to be an all-powerful "big brother". In addition, the resources of organised crime have also increased, requiring more effective methods of combating it. Commercialisation should be added as another element that represents a danger

to the protection of human personality[32].

Technological advancements have made visible the legal tolerance of invasions of privacy in connection with current considerations regarding the regulation of automatic data processing. Thus, in the years 1965-66, the US House of Representatives held a comprehensive hearing on computers and invasion of privacy, which resulted in several critical legislative initiatives. Similar debates can be noted in some Western European countries, which later resulted in the adoption of laws aimed at creating guarantees of informational privacy in the computerised era. One of the first data protection laws of this type, passed in Hessen in 1970, contained the characteristic provision that records, data and results covered by data protection must be acquired, transmitted and stored in such a way that they cannot be viewed, changed, extracted or destroyed by an unauthorised person. The period of the first wave of adoption of personal data protection acts spanned the period 1970-2010 on a global scale. For this legislation, data privacy is an aspect of data protection that deals with the proper storage, access, preservation, immutability and security of sensitive data.

The synergy of the wired world and artificial intelligence technologies has sparked a global privacy movement that has resulted in a new wave of regulation. As Lauren H. Rakower has written, in a world where the click of a button in one country can change a person's life in another, there needs to be a commitment to coordinate solutions that universally respect the right to privacy in the face of advances in technology[33]. An example of how this view has manifested itself in political practice can be the European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement (2016/2225(INI)). The resolution stated that the progress of communication technologies and the ubiquitous use of electronic devices, monitoring gadgets, social media, web interactions and networks, including devices which communicate information without human interference, have led to the development of massive, ever-growing data sets which, through advanced processing techniques and analytics, provide unprecedented insight into human behaviour, private life and our societies. The European Parliament has, therefore, called for the use of privacy by design and default, anonymisation techniques where appropriate, encryption techniques, and mandatory privacy impact assessments.

Westin's concept of freedom and privacy was associated with the fact that a person has control over information about himself. This theory needed to provide a clearer picture of both the degree of power and the kind of personal information one could expect to have control[34]. Michael Eldred foreshadowed it with a witty idea that freedom in the cyber world is, in the first place, a freedom for the cyber world itself to unfold its digital powers of control over changes within and without the digitised electromagnetic matrix. In this context, informational privacy is a superficial misnomer for the concealment of a personal world. The cyberworld, with its digital technologies, brings about a qualitatively new phenomenon of calculable cyber-disclosure of individual lifeworld that represents a danger to the freedom of a private individual to withdraw from the public gaze. This is akin to having one's movements through public streets automatically recorded, and a computer later analyses these data[35].

Automatic data processing is the skeleton of a smart city. So, it is not surprising that the intention to create information legislation for the new generation met with efforts to reconsider the concept of smart cities about ten years ago. In 2013, Adam Greenfield published an influential pamphlet in which he summarised the fundamental reservations about the smart city concept, primarily from an urban planning perspective[36]. He explained that the intense involvement of large commercial actors in the germination of ideas about urban design makes it seem as if urban thinking was inspired by United States Steel or General Motors rather than Le Corbusier or Jane Jacobs. It wasn't a unique old-fashioned sight. According to Greenfield, the same technology that underlies centralised computer management can be used for much more fruitful purposes.

In the technocratic mindset, smart cities focused on smart people should be feared. In the technocratic mindset, smart cities were supposed to be about smart people. The essential factors for building smart people are agreeableness, conscientiousness, emotional stability, extraversion and experience to openness[37].

Will there be enough smart people for smart cities? This approach is still warned in public debate, as Jagdish R. Sharma does, for example: «*If anyone fails to be intelligent enough to cope with the technology, then the very idea of Smartness is defeated. Careless and unintelligent people cannot handle the system*»[38]. The willingness of city dwellers to accept the processing of personal data fluctuates.

This is evidenced by regular surveys of the International Institute for Management Development in cooperation with the World Smart Sustainable Cities Organization. In response to the question "are you willing to concede personal data in order to improve traffic congestion?" answered positively (agree or strongly agree), for example, 91% of respondents in Hanoi, 63% in Geneva, 51% in Paris, and 35% in Tokyo. Different scores can be seen in the answer to the question "do you agree with facial recognition technology to reduce crime?", where e.g. 88% of respondents in Dubai, 77% in Beirut, 66% in New York and 57% in Amsterdam answered in the affirmative way[39].

The project Humane Smart Cities, which uses the power of technology only in direct connection with the needs and interests of residents, tried to ward off doubts[40]. Most recently, we have even met the More-than-Human project, creating a socially and ecologically just hybrid space in which people live in symbiosis with nature[41].

Parallel to the concept of smart cities, considerations of slow cities have attracted attention, aiming to create an alternative community design. The underlying idea was that even large cities can sustainably slow down their development[42].

In this context, we are interested in "more-than-human" data interactions, which move the design of smart cities away from the controversial idea of a human being inherently fused with data communication. As reminded by Crabtree et al., the acceptability and adoption of new technologies turns on their ability to be woven into the most mundane of acts. If they can't then they ultimately fail[43]. Regulation of personal data protection and institutional supervision would hardly produce this effect.

This way, we are returning to how Henri Lefebvre understood "Le Droit à la ville": «*the right to the city cannot be conceived of as a simple visiting right or as a return to traditional cities. It can only be formulated as a transformed and renewed right to urban life (...) it gathers the interest (overcoming the immediate and the superficial) of the whole society and, firstly, of all, those who inhabit it*»[44].

Even as the smart city becomes more human and environmental, data privacy is still a messy concept, no matter what happens. Woodrow Hartzog explains: «*There is now too much data that is collected by too many different entities and used in too many different ways for any singular definition of privacy to be legally useful anyway*»[45].

5. Conclusions

No security without privacy. This is how B. Fabrègue and A. Bogoni clearly titled one of the chapters of their study[46]. The same conclusion can be reached when looking at personal data protection. We live in an age where people cannot simply retreat to privacy by refusing to use specific technology because the infrastructure surrounding them is based on surveillance and automated indiscretion.

Emphasising ownership of personal data and mandatory consent shifts responsibility for the collective situation to the individual. Disposable digital identities allow residents to feel safe because they have choice and access, which are essential elements for a balanced community[47].

The difficulties of engaging in a smart city can hardly be overlooked. Smart city personal data vaults could potentially give city residents back control over their data. In times of profound change and great uncertainty, this could be a way to balance the issues of global distrust and the dark side of technology[48].

Data privacy guarantees allow people to benefit from innovative city services without fear of unnecessary disruption or bias. Inhabitants are more likely to embrace innovation if they are confident that their data will be handled responsibly and in their best interests[49].

1. This article was written under the umbrella of the 4 EU+ "*Chartering the course towards a legal framework for smart cities*" (reg. č. MA/4EU+/2024/F3/04).
2. J. Jacobs, *The Death and Life of Great American Cities,* Random House, New York, 1961, p. 58.
3. J. Jacobs, *Dark Age Ahead,* Random House, New York, 2004, p.175.
4. M. Vallianatos, *How LA Used Big Data to Build a Smart City in the 1970s,* in *Gizmodo*, June 22, 2015, https://gizmodo.com/uncovering-the-early-history-of-big-data-in-1974-los-an-1712551686.
5. J. Morris*, The Know-How City*, in *Destinations: Essays from Rolling Stone*, Oxford University Press, 1982, pp. 81-100.
6. M. Christodoulou, *Technopolis as the Technologized Kingdom of God*, in *Cahiers d'Études Germaniques,* 74, 2018, p. 126.
7. See H. Molotch, *The City as a Growth Machine: Toward a Political Economy of Place*, in *American Journal of Sociology*, 82, 2 (Sept. 1976), pp. 326-329.
8. See A. Glasmeier, S. Christopherson, *Thinking about smart cities,* in *Cambridge Journal of*

Regions, Economy and Society, 8, 2015, pp. 3-12.
9. M. Wakelin, *Globalization of Regional Development*, in D. V. Gibson, G. Kozmetsky, R. W. Smilor (Eds.), *The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks*, Rowman&Littlefield, New York, 1992, p.50.
10. A. Aurigi, S. Graham, *Virtual cities, social polarization, and the crisis in urban public space*, in *Journal of Urban Technology*, 1, 1997, pp. 15-17.
11. A. Mahizhnan, *Smart cities. The Singapore case*, in *Cities,* 1, 1999, p. 18.
12. L. Mora, R. Bolici, M. Deakin, Mora, L., *The First Two Decades of Smart-City Research: A Bibliometric Analysis*, in *Journal of Urban Technology*, 1, 2017, p. 4.
13. See T. Alizadeh, *An investigation of IBM's Smarter Cites Challenge: What do participating cities want*, in *Cities*, 63, 2017, pp. 170-180.
14. M. Foucault, *Space, Knowledge, and Power*, in P. Rabinow (Ed.), *The Foucault Reader*, Pantheon Books, New York, 1984, pp. 255-256.
15. D. Marongiu, *The Ideal City: Space and Time (from the Renaissance to Smart Cities)*, in *European Review of Digital Administration and Law*, 1, 2021, p. 17.
16. J. Berman, D. Mulligan, *Privacy in the Digital Age: Work in Progress*, in *Nova Law Review*, 2, 1999. p. 552.
17. W. T. DeVries, *Protecting Privacy in the Digital Age*, in *Berkeley Technology Law Journal*, 1, 2003, p. 309.
18. B. Periñán, *The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*, in *American Journal of Legal History* 2, 2012, pp. 189-190.
19. M. Korpiola, *Early Modern Swedish Law and Privacy: A Legal Right in Embryo*, in M. Green, L. C. Nørgaard, M. B. Bruun (Eds.), *Early Modern Privacy*, Brill, Leiden, 2022, pp. 135-136.
20. J. Locke, *Two Treatises on Government*, London, 1690, p. 216.
21. J. Yates in *Millar v. Taylor,* 20 April 1769, 4 Burr. 2378-2379, 98 E.R. 201.
22. See O. Kerr, *The Digital Fourth Amendment: Privacy and Policing in Our Online World*, Oxford University Press, 2024.
23. T. M. Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, Callaghan and Company, Chicago, 1879, p. 29.
24. S. D. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 5, 1890, p. 195.
25. See W. L. Prosser, *Privacy*, in *California Law Review*, 3, 1960, pp. 383-423.
26. See D. S. Papp, D. S. Alberts, A. Tuyahov, *Historical Impacts of Information Technologies: An Overview*, in D. S. Alberts, D. S. Papp (Eds.), *The Information Age: An Anthology on Its Impact and Consequences*, Washington, 1997, p. 14.
27. See S. Brand, *We Owe It All to the Hippies*, in *Time Magazine*, 12, 1995.
28. F. Turner, *From counterculture to cyberculture: Stewart Brand, the Whole Earth network, and the rise of digital utopianism*, The University of Chicago Press, 2006, p. 121.
29. A. Downs, *A Realistic Look at the Final Payoffs from Urban Data Systems*, in *Public Administration Review*, 3, 1967, p. 204.

30. B. Hoanca, *If Privacy Is Dead, What Can We Do Instead?*, in *IEEE Technology and Society Magazine*, 1, 2016, p. 37.
31. Alan F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967, p. 5.
32. S. Strömholm, *Right of Privacy and Rights of the Personality*, in *Acta Instituti Upsaliensis Iurisprudentiae Comparativae*, 8, 1967, pp. 18, 60-61.
33. L. H. Rakower, *Blurred Line: Zooming in on Google Street View and the Global Right to Privacy*, in *Brooklyn Journal of International Law*, 1, 2011 p. 347.
34. See H. T. Tavani, *Informational Privacy: Concepts, Theories, and Controversies*, in K. E. Himma, H, T. Tavani (Eds.), The Handbook of Information and Computer Ethics, Wiley, 2008, pp. 131-164.
35. R. Capurro, M. Eldred, D. Nagel, *Digital Whoness. Identity, Privacy and Freedom in the Cyberworld*, Ontos, Frankfurt, 2013, pp. 150, 158-159, 162-163.
36. A. Greenfield, *Against the smart city*, in *Do projects*, New York, 2013.
37. See C. Mun Chye, M. Fahmy-Abdullah, S. F. Sufahani, M. K. Bin Ali, *A Study of Smart People Toward Smart Cities Development*, in M. S. Kaiser, K. Ray, A. Bandyopadhyay, K. Jacob, K. Sie Long (Eds.), *Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering TCCE 2021*, Springer Nature Singapore Pte Ltd., 2022, pp. 257-272.
38. J. R. Sharma, *Smart people make a Smart City*, in *Daily Excelsior* (newspaper published in Jammu), 3. 8. 2024.
39. A. Bris et al., *Smart City Index 2024*, World Competitiveness Center, 2024, https://issuu.com/docs/e7a60c053affbf9e98fcba93afe857af?fr=xKAE9_zU1NQ.
40. See A. Oliveira, M. Campolargo, *From Smart Cities to Human Smart Cities*, in *48th Hawaii International Conference on System Sciences (HICSS)*, 2015, pp. 2336-2344; G. Concilio, F. Rizzo (Eds.), *Human Smart Cities*, Springer International Publishing Switzerland, 2016; E. Costa, A. Oliveira, *Humane Smart Cities*, in R. Frodeman (Ed.), *The Oxford Handbook of Interdisciplinarity*, Oxford University Press, 2017, pp. 228-240.
41. See J. Turner A. Morrison, *Designing Slow Cities for More Than Human Enrichment*, in *Multimodal Technologies and Interaction*, 1, 2021, p. 1-12; S. Heitlinger, M. Foth, R. Clarke (Eds.), *Designing More-than-Human Smart Cities: Beyond Sustainability, Towards Cohabitation,* Oxford University Press, 2024.
42. See H. Mayer and P. L. Knox, *Slow Cities: sustainable places in a fast world*, in *Journal of Urban Affairs*, 4, 2006, pp. 321-334.
43. A. Crabtree, T. Lodge, N. Sailaja, A. Chamberlain, P. Coulton, M. Pilling, I. Forrester, *Experiencing the future mundane: configuring design fiction as breaching experiment*, in *International Journal of Human–Computer Interaction*, 12.3.2025, https://doi.org/10.1080/07370024.2025.2454555.
44. H. Lefebvre, *Writings on Cities*, Blackwell, Oxford 1996, p. 158.
45. W Hartzog, *What is Privacy? That's the Wrong Question*, in *The University of Chicago Law Review*, 1, 2021, p. 1688.
46. B. Fabrègue, A. Bogoni, *Privacy and Security Concerns in the Smart City*, in *Smart Cities*,

1, 2023, p. 598.

47. See R. van Kranenburg, L. Anania, G. Le Gars, M. Arniani, D. Fantini van Ditmar, M. Kaili, P. Kavassalis, *Future Urban Smartness: Connectivity Zones with Disposable Identities*, in J. C. Augusto (Ed.), *Handbook of Smart Cities*, Springer Nature Switzerland AG, 2021, pp.1259-1284.
48. See H. S. Sheombar, J. V. Sheombar, *Peril on the Road to Utopia. Opportunities and Risks of Infusing Personal Data into the Smart City Ecosystem*, in S. Topham, P. Boscolo, M, Mulquin (Eds.), *Personal Data-Smart Cities*, River Publishers, Gistrup, 2022, pp. 5-23.
49. See Ch. Riedmann-Streitz, N. Streitz, M. Antona, A. Marcus, G. Margetis, S. Ntoa, Pei-Luen Rau, E. Rosenzweig, *How to Create and Foster Sustainable Smart Cities? Insights on Ethics, Trust, Privacy, Transparency, Incentives, and Success*, in *International Journal of Human–Computer Interaction*, 27.3.2024, https://doi.org/10.1080/10447318.2024.2325175.

Artificial Intelligence, Urban planning and the (Right to) Housing in Smart cities

Julio Ponce Solé

DOI: 10.13130/2723-9195/2025-1-81

L'analisi considera il ruolo dell'intelligenza artificiale (IA) in relazione alle smart cities. Le città europee utilizzano sempre più spesso l'IA per lo sviluppo di città intelligenti. Tuttavia, insieme ai suoi indubbi benefici, devono essere considerati anche i rischi che l'IA presenta. Il contributo analizza il possibile utilizzo dell'IA nel campo della pianificazione urbana e dell'edilizia abitativa e conclude considerando i limiti legali all'uso dell'IA nelle città intelligenti e la necessità di stabilire una riserva di umanità, cioè una riserva agli esseri umani di determinate decisioni, come già stabilito da varie legislazioni nazionali e dal regolamento UE sull'IA del 2024 per quanto riguarda le decisioni giudiziarie.

This analysis considers the role of Artificial Intelligence (AI) in relation to smart cities. European cities are increasingly using AI for the development of smart cities. However, the risks that AI presents need to be considered alongside its undoubted benefits. The paper analyses the possible use of AI in the framework of urban planning and housing and concludes by considering the legal limits of the use of AI in smart cities and the need to establish a reservation of humanity, i.e. a reservation of certain decisions for human beings, as already established by various national legislation and the EU AI regulation of 2024 in regard to judicial decisions.

1. Introduction: Aim of This Analysis

Public administrations are increasingly using AI to develop public policies in cities[1], even going so far as to adopt formal legal decisions in a fully automated way, as happened in late 2023 in the world-famous case of the Brazilian city of Porto Alegre, which passed a water meters ordinance entirely written with generative AI[2].

The purpose of this study is to analyse the use of AI in smart cities, considering its possibilities and its legal limits.

The OECD defines smart cities as «*initiatives or approaches that effectively leverage digitalisation to boost citizen well-being and deliver more efficient, sustainable and inclusive urban services and environments as part of a collaborative, multi-stakeholder process*»[3]. According to an EU study, «*Smart cities are therefore at the interface between social and technological dimensions*»[4].

The technological dimension of the smart city relates to the role of AI: «*While urban and local authorities can resort to AI to improve the efficiency of a given decision-making process or enhance the delivery of a public service, AI makes the most of its potential in a smart-city environment. The combination of AI and other digital technologies (big data, Internet of Things, cloud and telecommunication infrastructure) enables the development of smart cities*»[5].

Machine learning AI can be of great use to process big data and automate city management and make it more efficient in various areas such as public service provision (e.g. emergency services), environmental control, traffic, etc. In this study, I aim to concentrate on what could be called smart urban planning and management, and smart housing and homes.

In relation to local formalised legal decisions, legal rules such as urban planning or ordinances, and administrative acts such as traffic sanctions or building permits, AI can also play a relevant role, although, as will be briefly highlighted later, the law imposes certain legal limits on its use due to its potential risks.

In this sense, to conclude this introduction, the idea that we would like to highlight is the following. While AI has a number of important advantages for the promotion of the right to good administration of people living in cities (art. 41 of the European Charter of Fundamental Rights, ECFR[6], and national legislation of member states, e.g. art. 97 of the Italian Constitution or art. 30 of

the Statute of Autonomy of Catalonia), it also presents a number of environmental costs and risks to people's rights.

The advantages of AI have been highlighted by scholarship and jurisprudence[7]. Among those who write on the subject, it has been pointed out how AI is capable of processing huge amounts of data, making predictions using correlations, avoiding cognitive biases and what is known as "noise"[8], or generating new employment opportunities.

For example, in Italy, the decision of the Italian Council of State of December 13, 2019 (number 8472), underlines that (English translation is mine):

«*7.1 In general terms, it should be stressed that the public administration must also be able to exploit the considerable potential of the digital revolution. In this context, the use of computer algorithms for decision-making in the public and private spheres is based on the claimed gains in terms of efficiency and neutrality. In many fields, algorithms promise to become the tool through which the distortions and imperfections that typically characterise the cognitive processes and choices made by human beings, highlighted, especially in recent years, by an impressive range of literature on behavioural economics and cognitive psychology, can be corrected. In this context, the decisions made by the algorithm thus assume an aura of neutrality, the result of aseptic rational calculations based on data*».

Likewise, the decision of the same body of 4 February 2020 (number 881), stresses that (translation is mine):

«*As already highlighted in the previous section, the usefulness of this operational method of public interest management is particularly evident about procedures, such as the one at issue in this litigation, which are serialised or standardised, involve the processing of large numbers of applications, and are characterised by the acquisition of certain and objectively verifiable data and the absence of any discretionary appreciation. The full admissibility of these instruments is in line with the canons of efficiency and cost-effectiveness of administrative action (Article 1 of Law No. 241 of 1990), which, in accordance with the constitutional principle of good administration (buon andamento) (Article 97 of the Constitution), require the administration to achieve its objectives with the least expenditure of means and resources and by streamlining and accelerating the procedure*». However, along with the undoubted advantages of AI, scholarship and case law have also highlighted the risks that can arise with the use of this technology. From bugs

that can give rise to serious errors on an enormous scale, to biases, with the consequent danger of discrimination, adding the opacity generated by black boxes or the hallucinations that these systems can suffer, for example, which, on the other hand, will generate a replacement of humans in the workplace in both the public and private sectors.

Several judgments in different countries have identified a variety of problems related to the use of AI that have led to serious damage and public administrations being held responsible.

In the Australian case called "Robodebt", certain administrative tasks in the social field performed by humans were automated. The result of automation errors has been 400,000 welfare recipients in Australia who were wrongly accused of misreporting their income to the welfare agency and were consequently fined. From July 2015 to November 2019, the system used algorithms to calculate overpayments, collecting more than $1.2 billion, which the government will be forced to repay, because of a 2019 court ruling that the scheme was unlawful[9].

In France, the judgment of December 7, 2022 of the Paris Administrative Court annulled a decision to assign a student to a secondary school which was only the sixth option entered by the student in the "Affelnet" application, on the grounds that the methods of calculation of the student's points scale were incorrect and that these "material errors" influenced the overall line of the decision issued by the preparatory commission for the process and, consequently, the assignment decision taken by the academic director of the National Education Services[10].

In a British case, between 1999 and 2015, the British Post Office accused nearly 4,000 workers of theft, fraud and false accounting, of whom nearly 900 were convicted of crimes they did not commit, and which have been attributed to an error in the company's computer system. The case generated great suffering, including several suicides by those affected and even prison sentences, and has given rise to a television series, "Mr. Bates vs the Post Office" on the ITV channel.

In Spain, the ruling of December 30, 2021 of the Central Contentious-Administrative Court No. 8, which is the first judicial decision, except for errors or omissions, in relation to an algorithmic system in Spain, and the ruling of the National High Court of April 30, 2024, appeal no. 51/2022, which resolves the appeal against the former, have denied the access to the source code of the Bosco

program used by the Spanish Administration to solve applications to obtain the energy bonus in case of energy poverty. The litigation has arrived in 2024 to the Spanish Supreme Court which will decide in the future about this conflict definitively.

Therefore, the use of AI in smart cities by the authorities will always be double-edged: the improvements in public management (effectiveness of the right to good administration of people living in cities) vs. the risks of violating rights such as equality, transparency or data protection and privacy, for example. Hence the need for regulation of the use of AI, such as that developed by the Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (also known as Artificial Intelligence Act, RUEAI) and those that may be approved in the future by national public authorities to protect said rights.

2. Artificial Intelligence and Urban Planning

There is no doubt that one of the areas of competence of national local authorities in Europe is that of urban development and housing[11]. Decisions on land use and the location of housing and public and private infrastructures are of crucial importance in cities.

According to the above-mentioned EU study of 2021, there is evidence that smart cities that use AI are growing fast, in particular, after the COVID-19 crisis, although aggregate quantitative evidence is difficult to collect, in part due to the multiplicity of the forms smart cities can take, alongside their very varied use of AI. However, qualitative evidence from specific examples shows that the use of AI by local urban authorities is still mostly restricted to simple tasks. In general, incremental approaches are adopted to gradually develop initiatives and capacities around AI. There are interesting examples of larger and/or high-income cities, which have been early adopters of the smart-city concept, and which exhibit significant progress in the diffusion and exploitation of AI.

A field where several cities are working intensively is that of digital twins: digital

reproductions of the urban fabric of cities where cities can experiment with different public policies (e.g. traffic and transport policy)[12].
In general, the use of AI in the field of urban planning can be developed in several areas, for example:
(a) Analysis of big data: which makes it possible to know the urban situation of the city and proceed to develop actions against problems such as urban segregation caused by gentrification and exclusionary zoning.
b) The promotion of citizen participation in urban planning, as highlighted by Professor Rangone in relation to regulation in general[13].
This use of AI to support or assist urban planning decisions makes it possible to improve management and, as said before, to make the right to good administration effective in the urban planning sphere. The question to ask is whether AI could go beyond helping or supporting human decision-makers (e.g. mayors or town councils) to make the decisions for which they are responsible, but also directly take the decision in question, with a total automation of the urban planning procedure. In several European cities, for example, work is underway to use AI to fully automate the procedure for granting building permits[14]. I will return to this issue shortly.

3. Artificial Intelligence and (the right to) Housing

Having analysed some of the possibilities of AI in the field of urban planning, in this section we turn specifically to the use of this technology in relation to housing, which is considered a fundamental right by the European Court of Justice[15] and a right, even a constitutional right[16], in several European countries.
Again, AI can have several interesting applications here[17]. For example:
a) Identification of risks of disaster and disaster prevention.
b) Improving the management of the public housing service (or in EU terminology, service of general interest, used by national legislation, e.g. Spanish Housing Act 2023, art. 4): there are experiences in this sphere in the field of care for homeless people, for example[18].
c) Automation of homes: domotic or smart housing can enable elderly people to stay in their homes (ageing in place[19]) and save on energy consumption by improving the energy efficiency of buildings[20].

d) Law enforcement: in relation to inspections and detection of infractions in fields such as, for example, the tourist use of dwellings, a field where several Spanish cities are using AI[21].
In this field, it is worth highlighting the approval of Regulation (EU) 2024/1028 of the European Parliament and of the Council of 11 April 2024 on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724 published in the Official Journal of the EU on 29 April 2024. It entered into force 20 days later and will start to be applied from May 20, 2026.
This European regulation establishes several obligations on both hosts and short-term rental platforms. Hosts must apply to the authorities for a registration number. Once obtained, hosts must give this number to the platforms, which will provide the authorities with the data relating to the host's activity. With the information they can gather, the authorities will be able to assess the situation and apply the necessary public policies.
e) The application of AI in relation to housing also has its dark side, as it can lead to discrimination against tenants in the rental market. In the USA, tenant screening companies which screen possible tenants on the behalf of landlords or landladies (credit history, previous evictions, criminal record...) are becoming more and more frequent. That use of AI can create problems in the case of incorrect information containing errors, if irrelevant data are used or different treatment depending on race is implemented. The US Administration has issued in 2024 guidelines on the application of equal protection rights existing in US law in relation to this activity[22] and several cases have already reached the US courts[23].

4. Legal Limits to artificial intelligence in Smart Cities: the "*Humanity Reserve*"

Throughout this study we have pointed out the possible legal limits to the use of AI in smart cities in relation to urban planning and housing decisions. It's now time to address this issue directly.
Is it legally possible to use AI to fully automate administrative procedures related to urban planning and housing? In other words, is it possible to think of an AI

system that directly adopts an urban development plan or denies planning permissions?

The answer to this question is, in our opinion, that it depends on the type of legal decision to be taken and the type of AI to be used.

In the case of the use of AI to develop binding powers, there does not seem to be a major legal problem. This could be the case, for example, for building permits if there is no administrative discretion.

In relation to fully automated decisions in the field of discretionary powers, the question changes. The exercise of planning discretion implies a margin of appreciation, a volitional sphere, in which it is necessary, in accordance with the right to good administration and existing case law, to exercise due diligence and due care to take the best possible decision, considering all relevant factors and disregarding irrelevant ones[24]. Therefore:

1. When using rule-based systems of AI (simple/deterministic AI) that develop deductive inferences: it is not possible to eliminate discretionary powers if they exist, due to the prohibition of fettering by the right to good administration[25].

2. In the case of AI using statistics (complex/predictive AI) that develop inductive inferences (e.g. machine learning, deep learning): AI has no empathy, whilst being human is having the capacity to feel (some) identification with other humans (except psychos). It is true that AI can imitate empathy (like psychos), but it does not have mirror neurons, and it is not capable of developing real empathy[26].

It implies that AI cannot exercise the margin of appreciation existing in discretionary powers in a proper way, because it cannot take into consideration all the relevant factors, including the situation of the humans affected by its decisions.

3. Moreover, AI cannot make abductions, that is thinking like human beings with common sense and developing hypotheses. Abduction is a form of reasoning in which assumptions are made to explain observations. For example, if an agent were to observe that a light was not working, they can hypothesise what is happening in the world to explain why the light was not working. An intelligent tutoring system could try to explain why a student gives certain answers in terms of what the student understands and does not understand.

The term abduction was coined by Peirce (1839-1914) to differentiate this type

of reasoning from deduction, which involves determining what logically follows from a set of axioms, and induction, which involves inferring general relationships from examples[27].

4. Therefore, due to both factors, using AI for developing discretionary powers would be a violation of the right to good administration.

5. In the case of discretionary and binding powers, the principle of *audi alteram parte* included in art. 41 of the ECFR and in national legislations avoids a complete automation of administrative procedures since citizens must have the opportunity to be heard and to have their points of view considered by the public administration.

6. On the other hand, the duty to give reasons (also included in art. 41 of the ECFR and national legislations and now in art. 86 RUEIA regarding explainability, a component of the reasons)[28] is violated if AI systems that are black boxes are used.

In 1976 Weizenbaum (a MIT scientist) called for a societal consensus that machines should not replace humans in work that benefits from wisdom and empathy, a state that a computer would be unable to have (but might mimic emotions like psychos). In that sense, drawing on the work of other contemporaries looking at specific instances in which AI would be inappropriate, Weizenbaum named the following as roles that ought to be fulfilled only by humans: customer service representatives, therapists, eldercare workers, soldiers, judges and police officers. I think that Weizenbaum felt short with this list: actually, beyond certain jobs, any kind of exercise of administrative discretion should be in the hands of human beings due to the reasons exposed.

We can find several examples of a "reserve of humanity" established by law:

a) National level

German Administrative Procedures Act (*VwVfG*), Section 35a, fully automated issuing of an administrative act: «*An administrative act may be adopted entirely by automatic bodies, provided that this is permitted by law and that there is neither a discretion nor a margin of appreciation*».

Administrative procedure Catalan Act 26/2020, Article 44 about Automated administrative action: «*2. Only those acts that may be adopted with programming based on objective criteria and parameters shall be subject to automated administrative action*».

Spanish Charter of Digital Rights of 2021: «*XVIII.6 Efforts shall be made to promote citizens' rights as regards artificial intelligence recognised in this Charter in the framework of administrative action, recognising in all cases the rights to: decision-making being reserved to persons, in the absence of legislation providing for the adoption of automated decisions with the necessary guarantees*».

b) EU level

Art. 22 GDPR "Automated individual decision-making, including profiling": «*1. The 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.*

2.Paragraph 1 shall not apply if the decision:

A) is necessary for entering, or performance of, a contract between the data subject and a data controller.

B) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

C) is based on the data subject's explicit consent.

3.In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4.Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place».

The EU regulation on AI of 2024 (REUAI) prohibits its use in some cases included in art. 5 (unacceptable risks), but no mention is made to administrative discretionary powers. However, in relation to judges, Annex III of the REUAI states that high-risk AI uses include:

«*8. Administration of justice and democratic processes: (a) AI systems intended to assist a judicial authority in the investigation and interpretation of facts and law, and in the application of the law to a particular set of facts*».

Recital 61 REUAI indicates that «*The use of AI tools can support the decision-*

making power of judges or judicial independence but should not replace it: the final decision-making must remain a human-driven activity».

In relation to executive power, Annex III of the REUAI establishes that high-risk AI uses include «*AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status*». In that case it could imply that AI systems can only assist decision-makers, not replace them. But in other references in Annex III this distinction is not so clear (e.g. «*Migration, asylum and border control management*»).

It is possible to consider the possibility of extracting a principle from Annex III interpreting words such as "assist", "evaluate", "establish priorities" in the sense that machines should be a supporting tool provided there is discretion but not replace human decision-making. In any case, to avoid confusion, such a prohibition of replacing the final discretionary human decision should be explicitly included in the future, in my opinion, in art. 5 of the REUAI to make it clear and to cover other cases in which there is no specific high risk but rather administrative discretion, the use of which can, in itself, constitute a high risk of maladministration and violation of citizens' rights.

Therefore, in the current state of the art of AI, the precautionary principle and the legal limits seen above impose the avoidance of such uses of this technology in smart cities. Exclusion of fully automated discretionary decisions, taken only by AI, is not a consequence of technical reasons but of legal considerations.

5. Conclusions

As we have seen, AI could be a tool for good administration in the field of urban planning and housing. European cities are using AI increasingly in the context of smart cities. However, the fact that AI can be technically available to be applied in any area of administrative activity creating full automation does not mean it is always legally possible to do so. In this analysis we have discussed the need for a human reserve, that is, that some decisions (discretionary) in relation to some kinds of AI (rule based and non-symbolic) should be in the hands of human beings, due to legal considerations based on avoiding fettering and respecting the right to good administration.

I would like to finish by underlining that one of our big challenges ahead will be to be able to achieve the best from humans and the best from AI in the regulation of land use and housing and in the deployment of smart cities[29].

1. This study is a result of the research project PID2023-151396OB-I00 (*La mejora de las decisiones administrativas mediante el uso de IA, la experimentación y los* sandboxes*: especial atención al ámbito urbano y de vivienda*), funded by the Spanish Government.
2. See for example The Washington Post, 4 December 2023: «*A Brazilian city passed a law about water meters. ChatGPT wrote it*», https://www.washingtonpost.com/nation/2023/12/04/ai-written-law-porto-alegre-brazil/.
3. OECD, *Enhancing the Contribution of Digitalisation to the Smart Cities of the Future*, 2019: https://www.oecd-ilibrary.org/docserver/f6970913-en.pdf?expires=1733825724&id=id&accname=guest&checksum=90234C9A8259F0814115ABE4B0D6721B
4. European Parliament, *Artificial Intelligence and Urban Development*, 2021: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690882/IPOL_STU(2021)690882_EN.pdf.
5. European Parliament, *Artificial Intelligence and Urban Development*, 2021, p. 21.
6. Article 41, "Right to good administration": «*1.Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union. 2.This right includes: (a)the right of every person to be heard, before any individual measure which would affect him or her adversely is taken; (b)the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; (c)the obligation of the administration to give reasons for its decision. 3.Every person has the right to have the Union make good any damage caused by its institutions or by its servants in the performance of their duties, in accordance with the general principles common to the laws of the Member States. 4.Every person may write to the institutions of the Union in one of the languages of the Treaties and must have an answer in the same language*»
7. In general, see J. Ponce, *El Reglamento de Inteligencia Artificial de la Unión Europea de 2024, el derecho a una buena administración digital y su control judicial en España*, Marcial Pons, Madrid, 2024.
8. D. Kahneman, O. Sibony, C. Sunstein, *Noise. A flaw in human judgement,* William Collins, London, 2021.
9. Details available at: https://www.theguardian.com/australia-news/2020/may/29/robodebt-government-to-repay-470000-unlawful-centrelink-debts-worth-721m.
10. Details accessible at: https://www.actu-juridique.fr/administratif/des-erreurs-de-donnees-traitees-par-un-algori

thme-peuvent-etre-cause-dillegalite/.

11. However, the EU is increasingly intervening in this field, thanks to the impact of other EU powers on the cities. See J. Ponce, *The European union role in ensuring access to affordable housing and in fighting against urban segregation and gentrification: moving forward,* in *Journal européen des droits de l'homme = European journal of human rights*, no. 5, 2019, p. 311-334.
12. See in the case of Barcelona: https://eurocities.eu/stories/barcelona-shapes-the-future-of-city-planning/.
13. N. Rangone, *Artificial intelligence challenging core state functions. A focus on law-making and rule-making,* in *Revista de Derecho Público: Teoría y Método*, Vol. 8, 2023, pp. 95-126.
14. For the Vienna case https://digitales.wien.gv.at/en/projekt/brise-vienna/. In Spain, see the cases of Madrid or Vitoria: https://blogs.vitoria-gasteiz.org/medios/2024/07/04/el-ayuntamiento-recurrira-a-la-inteligencia-artificial-para-agilizar-la-concesion-de-licencias/; https://www.madrid.es/portales/munimadrid/es/Inicio/Actualidad/Noticias/Madrid-avanza-hacia-la-automatizacion-para-agilizar-la-tramitacion-de-licencias-urbanisticas/?vgnextfmt=default&vgnextoid=5dbcf5d9881bd810VgnVCM1000001d4a900aRCRD&vgnextchannel=a12149fa40ec9410VgnVCM100000171f5a0aRCRD.
15. Court of Justice, judgment 10 September 2014, Case C-34/13, KUŠIONOVÁ, ECLI:EU:C:2014:2189, paragraph 65: «*Under EU law, the right to accommodation is a fundamental right guaranteed under Article 7 of the Charter that the referring court must take into consideration when implementing Directive 93/13*».
16. E.g. Belgian Constitution, art. 23.3, Spanish Constitution, art. 47 or Finnish Constitution, chapter 2 Section 19.
17. See C. Compton and Jessie Hohmann, *AI and the Right to Housing*, in A. Quintavalla, J.Temperman (eds), *Human Rights and Artificial Intelligence: A Deskbook,* Oxford University Press, 2023.
18. H. Chan, E. Rice, P. Vayanos, M.Tambe, M. Morton, *Evidence From the Past: AI Decision Aids to Improve Housing Systems for Homeless Youth ,* in *Proc. of AAAI Fall Symposium Series on Cognitive Assistance in Government and Public Sector Applications*, 2017, https://teamcore.seas.harvard.edu/publications/evidence-past-ai-decision-aids-improve-housing-systems-homeless-youth-0.
19. RL, Fritz, G. Dermody, A *nurse-driven method for developing artificial intelligence in "smart" homes for aging-in-place.*, in *Nurs Outlook.* 2019 Mar-Apr, 67(2), p. 140-153.
20. R. O. Yussuf, O. S. Asfour, *Applications of artificial intelligence for energy efficiency throughout the building lifecycle: An overview*, in *Energy and Buildings,* Vol. 305, 15 February 2024.
21. For example, Valencia: https://inspain.news/valencia-on-the-hunt-for-illegal-tourist-apartments-with-ai-and-chatbots/.
22. US. Department of Housing and Urban Development, *Guidance on Application of the*

Fair Housing Act to the Screening of Applicants for Rental Housing, April 2024, https://www.hud.gov/sites/dfiles/FHEO/documents/FHEO_Guidance_on_Screening_of_Applicants_for_Rental_Housing.pdf.

23. See the American judicial decision *Conn. Fair Hous. Ctr. v. CoreLogic Rental Prop. Sols*, 478 F. Supp. 3d 259 (D. Conn. 2020), https://studicata.com/case-briefs/case/conn-fair-hous-ctr-v-corelogic-rental-prop-sols/ . SafeRent, an AI screening tool used by landlords, will no longer use AI-powered "scores" to evaluate whether someone using housing vouchers would make a good tenant. US District Judge Angel Kelley issued final approval for a roughly $2.3 million settlement to prevent SafeRent from discriminating against tenants based on income and race in November 2024, according to information included at https://www.theverge.com/2024/11/20/24297692/ai-landlord-tool-saferent-low-income-tenants-discrimination-settlement.
24. J. Ponce, *The Right to Good Administration and the role of. Administrative Law in promoting good government*, in A. Cerrillo, J. Ponce, *Preventing Corruption and Promoting good Government and Public Integrity*, Bruylant, p. 25 ff.
25. P. Craig, Administrative *Law*, Sweet and Maxwell, Thompson Reuters, 9th edition, 2021, paragraph 10-025.
26. C. Misselhorn, *'Empathetic' AI has more to do with psychopathy than emotional intelligence – but that doesn't mean we can treat machines cruelly*, in *The Conversation*, 21 March 2024, https://theconversation.com/empathetic-ai-has-more-to-do-with-psychopathy-than-emotional-intelligence-but-that-doesnt-mean-we-can-treat-machines-cruelly-225216.
27. See term abduction in the Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/abduction/peirce.html. https://artint.info/html/ArtInt_133.html. Also D. L. Poole & A. K. Mackworth, *Artificial Intelligence: Foundations of Computational Agents,* 3rd Edition, Cambridge University Press, 2023, https://artint.info/3e/html/ArtInt3e.Ch5.S8.html
28. Article 86, "Right to explanation of individual decision-making": «*1. Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken. 2. Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law. 3. This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law*».
29. As the great American computer scientist J.C. Licklider pointed out many years ago in his famous article *Man-computer symbiosis,* in *IRE transactions on human factors in electronics*, 1, 1960, p. 4-11.

Digitalisation of public administration under martial law in Ukraine and the case of Smart City Kyiv

Liliia Serhiichuk

DOI: 10.13130/2723-9195/2025-2-70

I cambiamenti evolutivi avvenuti in Ucraina negli ultimi decenni testimoniano la rivoluzione dell'informazione, che ha portato a tecnologie digitali progressive, nuovi prodotti e servizi. L'inizio dell'aggressione militare su larga scala della Federazione Russa contro l'Ucraina ha reso necessaria l'attuazione di misure di risposta rapida alle minacce esistenti e lo sviluppo di una strategia di digitalizzazione negli anni del dopoguerra. L'aspetto chiave di tali sistemi è la componente di sicurezza: il rilevamento e l'informazione tempestiva dei residenti sull'emergere di varie minacce legate all'aggressione militare, ecc. La guerra è ancora in corso in Ucraina, ma le città si stanno sviluppando tecnologicamente. Kyiv è la prima città in Ucraina a implementare sistematicamente tecnologie innovative e a creare attivamente l'infrastruttura digitale della città. Per capire meglio come vive un tipico kieviano durante la guerra, è necessario ricercare le principali innovazioni che usiamo ogni giorno e come la digitalizzazione è regolata a livello legislativo.

The evolutionary changes taking place in Ukraine over the past few decades testify to the information revolution, which has resulted in progressive digital technologies, new products and services. The beginning of the full-scale military aggression of the Russian Federation against Ukraine necessitated the implementation of rapid response measures to existing threats and the development of a digitalisation development strategy in the post-war years. Key aspect of such systems is the security component - the detection and timely informing of residents about the emergence of various threats related to military aggression, etc. While the war is still ongoing in Ukraine, the cities are developing technologically. Kyiv is the first city in Ukraine to systematically implement innovative technologies and actively create the city's digital infrastructure. To better understand how a typical Kyivan lives during the war, it is

necessary to research the main innovations that we use every day and how digitalisation is regulated at the legislative level.□

Summary: 1. Introduction.- 2. Digitisation of government processes in the international arena.- 3. Diia – the State of the smartphone.- 4. Kyiv Digital – the city in the pocket.- 5. Other digital services.- 6. Challenges and prospects.- 7. Conclusions.

1. Introduction

The acceleration of urbanisation[1], together with the rapid development and cheapening of ICT, led to the emergence of smart steel cities in the 1990s. This new approach means combining information and communication technologies with economic, political, and socio-cultural changes to solve urban problems.
Cities are trying to use this model as a possible way to overcome the challenges of urbanisation, such as lack of resources and infrastructure, urban overcrowding, increasing demand for health services, ageing populations in the "old world", and large numbers of young people in the population in developing countries, as well as environmental problems.
The need to create smart cities is a strategic step in the direction of development, which involves using modern technologies to improve the quality of life of citizens and support sustainable development. Smart cities provide an opportunity to enhance the efficiency of resource management, develop transport and communication infrastructure, provide affordable and high-quality services to residents, and increase the overall level of city intelligence.
According to UN forecasts, by the end of the 21st century, 84% of the population will live in cities. By 2025, the population in 34 cities will exceed 10 million people. Cities already consume 2/3 of the world's energy and most other resources. One can only imagine the impact on consumption in those cities with a population of more than 10 million people[2].
Ukrainian cities are no exception. About 68.8% of Ukraine's population lives in cities, which increases the pressure on the existing infrastructure[3]. The active development of digital society and the formation of the digital economy at the

stage of "Industry 4.0" led to a significant range of research devoted both to the overall process of digitalisation and its manifestation and practical aspects of implementation at the city level.

Today, many studies perceive the smart city as the most popular city and ideal, which is included in understanding the genesis and determination of the future of urbanised systems, the formation of new urban settlements, and the regeneration of existing ones[4]. In general, the concept of a smart city is closely related to the processes in the city and encourages people to behave accordingly and make rational decisions. The concept of a smart city has different interpretations. However, the general idea of an innovative city system is based on three simple principles: comfort, convenience, and safety of residents. Modern technologies and services are the primary means of helping create so-called smart cities. Smart and open management, a convenient and safe urban environment, advanced technologies, and citizens who contribute to the city's development are all signs of a smart city. D. Washburn and co-authors claim that the city makes "smart" by combining information and network technologies to improve services in governance, education, health care, public safety, construction, transport, and communal services. T. Shelton et al. perceive most smart city projects as clumsily integrated interventions into existing social and spatial structures of the environment[5]. The research topic is quite popular among the Western world's academic, business, and political circles. In particular, such well-known academic researchers as B. Cohen[6], R. Jiffinger and H. Gurdun[7], P. L. Lombardi[8], A. Murray, M. Minevych, and A. Abdulaev[9] contributed to the formation of the concept, the study of its components, and the interpretation of the definition. In addition, theoretical and empirical studies of smart cities are covered in the works of V. Albino, U. Berardi and R.M. Dangelico[10], J. Handrlica[11], M. Bernardo[12], A. Camero and E. Alba[13], J. Chen, Y. Guo, C. Su, J. Chen and S. Chang[14], M.J.N. Han and M.J. Kim[15], B.N. Silva, M. Khan and K. Han[16]. World organisations such as the European Commission, ITU, OECD, and UN-Habitat are engaged in developing principles, indices, and recommendations regarding the mechanism for implementing the concept in cities.

Digitisation of public services in the context of the democratic development of society has been a key trend in the public administration system in recent years.

Ukraine is marked by significant achievements in this field, occupying a high position among the most developed countries in the world. Nevertheless, the study of foreign experience in this direction is essential for the Ukrainian state, taking into account its aspirations for European integration.

In Ukraine, the study of this topic is just beginning to interest scientists. Most of the relevant works so far are related to electronic governance, which is only one component of a smart city. In particular, the digitisation of state services has been studied by many scientists, such as Yu. Danko and N. Bilotserkivska[17], L. Marchenko[18], H. Ortina and N. Rybalchenko[19], M. Polishko[20], O. Stogova and D. Murach[21], R. Frosinyak[22], I. Zhukovich[23], S. Chukut and V. Dmytrenko[24].

The issue of digitalisation of urban development, taking into account the world experience of implementing smart city strategies, particularly approaches to determining the level of digitalisation of the city, are considered in the scientific works of T. Pushkar. In these studies, the prospects for the selection of urban projects based on the Global Index of the Development of Smart Cities, the use of an interdisciplinary thinking approach to determine urban digitalisation projects based on the preferences of residents, and the assessment of the perception of innovative digital technologies by city residents[25], [26].

The problems of the formation and development of smart cities are focused on two main aspects: technological and technical components of digitisation and socio-economic foundations and consequences.

In terms of the first approach, I. Opirskyi and O. Tyutikov define a smart city as a structure that mainly includes information and communication technologies for the development, deployment and promotion of sustainable development practices to solve the problems of urbanisation[27]. Another approach focuses on sustainable development, which is determined by the factors that form each of the components of a smart city, providing a balanced combination of economic, social and environmental factors[28].

Ukrainian researchers such as I. Antoniuk and S. Koshova describe the domestic and foreign experiences of implementing smart-city programs in large cities[29]. I. Vorobyov and O. Shylo, consider the peculiarities of the stylistic combination of old and new architecture in the conditions of the post-war reconstruction of Ukrainian cities[30], L. Zhilinska, G. Kucherova and O. Tarasevich, who focus attention on the problems of applying the Smart-city concept to solving the tasks

of restoration and development of spheres of urban life in the post-conflict territories of Ukraine[31], O. Zakharova and D. Kozyrev, who see in the concept of the smart city an alternative approach to the restoration of the urban infrastructure of Ukraine in the post-war period[32], T. Palamarchuk, who examines the peculiarities of the development of smart cities under the influence of globalization processes[33], O. Palivoda and O. Bondarenko, who focus on European approaches to the marketing of smart cities[34], and N. Protsyuk, reveal the conceptual foundations of the interpretation of the essence of the smart infrastructure of cities in the context of sustainable development[35], K. Radchenko, who elaborates on the categorical and conceptual apparatus of the Smart-city concept[36], R. Sevastyanov, who outlines the current problems of the development of smart cities[37], I. Dunaev and N. Havkalov, who are developing a platform model of citizen participation within the framework of the smart-city concept for the cities of post-war Ukraine; M. Gramchuk and V. Nikitenko, whose participation outlines modern trends and prospects for the development of a smart city[38].

So, I. Dunaev, N. Havkalova and A. Kud emphasise that «*the concept of a smart city does not involve a simple replacement of social development with technological re-equipment of the urban space. The key feature of the concept is the direct participation of people in the processes of city management and, in particular, urban development*»[39].

In the conditions of economic transformation and the formation of an innovative digital society, Ukraine faces several significant problems and challenges in building smart cities. The concept of smart cities has gained a lot of popularity as people seek to solve the problems created by rapid urbanisation, resource constraints and technological advances. Smart cities use the power of data-driven technologies to optimise various aspects of urban life, including transportation, energy consumption, waste management, governance, and more. Determining the problems and challenges associated with the development of smart cities in Ukraine requires a systematic approach.

At the same time, I see the need for more active research on the topic since the process of building smart cities in Ukraine has already begun, and the academic sector should be one of the leading participants in the process. Currently, there is a lack of systematisation of foreign experience and proposals for Ukrainian cities,

which have been developed considering national characteristics.
It should be noted that Ukraine already has a particular system of essential legislation that ensures digitalisation. In particular, the Laws of Ukraine On electronic documents and electronic document management, electronic digital signatures, administrative services, etc. However, each new project and direction in this area entails the introduction of changes to the existing legislation and, in some cases, the adoption of a new normative legal act. Currently, several draft laws aimed at the development of digitalisation policy and strengthening of state regulations of this area have been registered.
Before the start of the full-scale aggression, Ukraine was one of the European leaders in terms of the level of development of the field of open data. Services based on them were used by about 7 million Ukrainians every month. Open data was the basis of anti-corruption policy and the main factor in the development of civil society, accountability and transparency of government. However, during the period of martial law, there was a temporary restriction of access to the National Open Data Portal to ensure the interests of national security. Post-war reconstruction should be carried out taking into account the requirements of the anti-corruption policy and complying with international standards of transparency and accountability.
Based on the above, the purpose of the article is to propose the improvement of the concept of smart cities in Ukraine and the digitalisation of public services in the context of the democratic development of society by analysing the shortcomings of digitalisation of the city based on the experience of the city of Kyiv, taking into account the experience of world cities and the national characteristics of the development of the city in the war and post-war periods.
This article also discusses the fact that each country has specific approaches to providing electronic services by state authorities. Therefore, it is important to carefully analyse how the digitalisation of public services is taking place worldwide and evaluate the advantages and disadvantages of existing models through the prism of the possibilities of their implementation in Ukraine.
Therefore, to achieve the goal, one of the key tasks in implementing innovative technologies is adapting global experience and best practices of building smart cities to the conditions of Ukrainian reality. First of all, it is important to consider the peculiarities of the economic, socio-cultural, and political situation in

Ukraine. The application of global experience should be based on a careful analysis of the country's context and needs. In this regard, the research topic devoted to the problems and prospects of digitalisation in Ukraine is relevant.

2. Digitisation of government processes in the international arena

The global experience of digitisation of government processes in the field of public service provision deserves special attention, as it emphasises the importance of digital technologies in public administration as a means of improving the efficiency, accessibility and quality of public services. Some countries note the apparent advantages of digitisation of public services but, at the same time, point to the challenges and problems that arise during their implementation. Considering the rapid development of technologies, there is a need for constant monitoring and updating of digitisation strategies in the context of changes in the technological, social and economic environment.

It is worth noting that the actual concept of a smart city - is that in such a city, most life processes are subject to the smart principle - that is, they are managed with the help of digital technologies and are, in one way or another, interconnected. A well-known expert in this field, Nikos Komninos, emphasises that «*a city can be considered "smart" if it invests in human and social capital and communication infrastructure for active promotion of sustainable economic development and high quality of life, including reasonable management of natural resources, through public participation*»[40].

The beginning of digitisation of public services was celebrated in Singapore. Since 1980, the government of this country has defined the task of implementing the Civil Service Computerization Program by the year 2000 (The Civil Service Computerisation Programm). As a result, the government portal www.gov.sg was launched in 1998 and is managed by the Public Communications Department of the Ministry of Communications and Information. It features announcements about the country's policies, current information and news, and public services for the population, such as a doctor's appointment, employment service, calling the police, changing the composition of the family, and others[41].

In 1999, the Canadian government launched the "Electronic Canada" (e-

Canada) initiative to provide citizens and businesses with quick and efficient access to the necessary information and improve the accessibility of government services in general. Today, the digital transformation of management processes is underway in Canada, and the government is actively implementing various initiatives, such as the "Cyber Security Strategy 2019-2024" and the "Digital Government Strategy 2021-2025". One of the examples of digitisation of public services in this country is the government project on the use of blockchain technologies in the field of forestry, with the help of which it is planned to improve the tracking of deforestation operations and the storage of important information about the state of forest resources[42].

Denmark is rightly recognised as one of the leading countries in Europe in the implementation of digital public services, and this achievement is partly explained by an active state policy in this area. The Danish government has set clear priorities for the implementation of digital public services, focusing on improving efficiency, simplifying regulations, providing better social services, and actively using new technologies to improve the quality of management in the public sector. Also, significant emphasis was placed on reducing bureaucracy by simplifying registration procedures and regulations, which allowed civil servants to have more time to perform essential tasks.

It is also worth considering the Estonian experience of digitisation of public services. This country is positioned among European countries as a leader in the implementation of electronic services among the population. The uniqueness of e-democracy in Estonia is that both state institutions and civil society were included in its formation. Authorities monitor, adapt, and bring about the development of the information society by following legislation and ensuring citizens' access to information resources. In modern conditions in Estonia, there are practically no public services that do not use elements of information and communication technologies.

It is interesting that back in 2005, local elections were held in Estonia, during which the possibility of electronic voting was introduced using a personal electronic identification card. The same technology was used in the parliamentary elections in 2007. As part of this process, the voter had the opportunity to cast his vote several times, but only the last vote was counted. During the first introduction of electronic voting in 2005, this service was used

by about 1.85% of voters. However, by 2011, this figure had grown to 25%, and in the 2019 elections, almost half of the voters used electronic voting[43].

Also, in Estonia, the government has created an electronic platform, www.eesti.ee, with the help of information technology, which provides access to various public services in one place, such as obtaining medical services, registering a business, paying taxes, etc. This contributed to the reduction of the level of corruption, effective interaction between the authorities and citizens, and the reduction of bureaucratic procedures. On a single portal, while receiving administrative services, the population can find relevant information and recommendations from various spheres of life, such as culture, sports and recreation, safety and protection, work and labour relations, health and recipes, family and many others[44].

The Estonian experience of digitising public services and the introduction of electronic voting is essential not only because it used this technology but also because it managed to attract a significant number of the population to it in a short period. Thus, this success in Estonia inspired many European countries, including France, the Netherlands, and Great Britain, to conduct similar experiments.

It should be noted that the concept and practice of smart-city project implementation have been quite successfully implemented around the world since the beginning of the 21st century. The most significant results are demonstrated by cities such as Zurich, Oslo, Canberra, Copenhagen, Helsinki, Geneva, Barcelona and Amsterdam. This experience is spreading rapidly among other cities in Europe and the world. In contrast, in Ukraine, the implementation of the concept of smart cities takes place on a point-by-point basis based on budget programs and projects[45]. Ukraine is not yet among the countries actively working on developments for smart cities.

Amsterdam is an example of a city combining top-down and bottom-up approaches. Although the development of the smart city of Amsterdam started back in 2009, it has not led to the adoption of a strategy; the process is still based only on individual program documents. However, in 2017, the National concept for the development of smart cities in the Netherlands was presented, combining the efforts of 40 representatives of local authorities, 30 scientists and 60 representatives from the business sector[46].

In particular, China leads in terms of the number of its inventions. However, the United States has the most extensive territorial coverage: patent documents of American inventors include 24 different jurisdictions. Great Britain, South Korea, Norway, India and Japan follow them. Telecom giants have taken the technological lead in smart cities in most countries. In the non-Chinese segment, Samsung ranks first in the number of patent families (a group of publications related to one invention). It is followed by the American Cisco, which specialises in the development of network equipment. Huawei and Xiaomi stand out among Chinese companies[47].

Cities typically start with separate smart city strategies, elements of which can then be integrated into an overall city development strategy. The strategy is then owned by those who provide services and manage city resources. As a rule, for such cities, the smart city model itself is not intended but rather a means to achieve other goals.

In some countries (Netherlands, Singapore), national strategies exist. Still, they do not override the rights of individual cities to create their products; they only aim to develop specific standards and ensure the exchange of knowledge and best practices between cities.

Most cities involve all interested parties in the development of strategies based on public-private partnerships, with citizens' active participation[48].

For organisation and management, it is standard to create a department for the development of a smart city under the municipality to combine the necessary efforts of all parties, use a private-public platform for interaction (Amsterdam, Vienna), start the position of the Head of Information and Cif-rotation (London), etc. In European cities, financing takes place at the expense of budget funds, namely the city budget, EU funds, and the national budget. In North America, private investment plays an important role.

Most smart cities launch a platform for interaction together with the strategy ("Amsterdam Smart City", "Vienna Smart City", "London Smart City Council", etc.). The platform is a platform for discussions and the development of ideas and also unites representatives of the government, business, civil society, and the academic sector. For the most part, innovative projects by direction are indicated on the websites of the Smart Cities platforms (Vienna, Amsterdam, Barcelona) or listed on the single city website (London, Stockholm). The solutions are divided

by directions (infrastructure and technologies, resources and «economy of the full cycle», mobility, education and governance, lifestyle, etc.) and correspond to the goals of the strategies.

The concept of digital sustainability, that is, the development of solutions that can be used effectively over a long time, is gaining significant importance. Such solutions are easy to modify, use, and combine with others[49]. The concept of smart cities has recently gained popularity in Ukraine for several reasons, such as the intensification of decentralisation processes, the large number of IT specialists, society's readiness for changes, and the formation of demand for them. In addition, implementing local initiatives is much faster and easier than within the framework of the entire country. The concept is most actively realised in Kyiv, Lviv, Kharkiv, Vinnytsia, and Dnipro. At the same time, about 15 cities in Ukraine use this concept to some degree, implementing innovative solutions. However, some features inhibit this process.

One feature of the implementation of the concept in Ukraine is the activity of the public and the "creative class" which often works on a volunteer basis and exclusively on enthusiasm.

Cities have the opportunity to use their funds, public-private partnership mechanisms, funds from EU sectoral budget support, and the State Fund for Regional Development. However, currently, only 30% of all projects submitted to the competition for state funding are city council projects[50]. Only one city, Kyiv, has officially adopted a Smart city strategy. Some cities demonstrate the desire for a purposeful strategic approach by creating Project offices (Kharkiv, Dnipro) and relevant positions, developing Digitalisation strategies (Lviv, Vinnytsia), starting forums for the exchange of experience ("Lviv Forum 451°E", "Kyiv Smart City forum"), etc.

In general, the global experience of digitising public services shows the importance of this direction in the development of public administration, which can lead to improvements in accessibility, transparency, and efficiency. The experience of developed countries such as Denmark, Estonia, Singapore, and many others shows what results the state can achieve by digitising its services.

A smart city strategy should be public and dynamic. It should include goals with a specific period for tracking progress and success criteria. The city should regularly publish updates and achievements on a specially created platform.

Experience shows that cities with a systematic approach and strategies better meet the needs of their residents than those that develop innovative applications on demand. Ukrainian cities are just beginning to use digitalisation's advantages and form their Smart strategies, so it is essential to set priorities correctly.

3. Diia – the State of the smartphone

The positive impact of digitalisation on the democratic development of society occurs because the digitalisation of all spheres of life in the country significantly changes social relations and legal regulation and creates new challenges and expectations. The digitalisation of public services is designed to ensure transparency, openness, control, and interaction between public authorities and the population, promote equality and justice, and support and develop democracy in general. The state should become a service, not a scary monster. It should help some get services quickly and others do their jobs honestly.

To turn Ukraine into an actual digital state, it is necessary to digitise many more services, update the legislative framework, streamline the work of state registers, and ensure technical capabilities and data protection. Changes affected administrative services, health care, business, education, transport, courts, issues of democracy, etc. Ukraine has become and continues to improve the concept of a digital state, which has components such as e-governance, cyber security, e-democracy, e-business, e-court, e-health, e-education, e-transport, smart cities, digital skills, and ubiquitous internet. In 2019, the government created the Ministry of Digital Transformation. This body forms and implements state policy in information society development, digital economy, e-government, e-services, digital innovations, and the IT industry.

Thanks to Ukraine's accession in September 2022 to the "Digital Europe" Program until 2027, significant achievements in digital transformation will take place. Six billion Euros will be allocated to Ukraine over seven years to finance projects in four areas: high-performance computing, artificial intelligence, data and cloud services, digital technologies in business and society, and digital skills. Ukraine is actively working in this direction, promoting the development of the digital economy and implementing the Diia application[7] which helps implement public services.

The Kitsoft company, commissioned by the Ministry of Digital Transformation of Ukraine, developed the most potent IT platform for state services, Diia, which the Ministry of Digital Transformation owns. The application that made millions of Ukrainians fall in love with digitisation, and now the world is falling in love. Now, Diia includes 94 projects. It is an automatic service without officials, opening a bank account in 5 minutes, and documents that are always on the smartphone. Ukrainians are already used to the fact that the most popular government services can be obtained in a few clicks, without queues and bribes.
«*Today, Diia is an application used by 18.7 million Ukrainians and has completely changed the perception of the interaction between the state and citizens. In three years, we launched 14 digital documents and more than 25 services in the application. Our team has dashboards that are convenient for tracking the number of people who have used the service. This tool allows you to analyse the service's demand and whether users are satisfied with receiving it in Diia. The most popular are digital documents. Ukraine became the first country in the world to have a digital passport with the same power as a paper or plastic counterpart. In total, in Diia, Ukrainians use 4.7 million ID cards, 12.2 million foreign passports and 6.6 million driver's licenses in the application. We are the fourth in Europe to have a digital driver's license. Drivers can pay fines in a few clicks or share a car with a relative or friend so that the technical passport appears in Diia*» emphasised the Minister of Digital Transformation[51].
Among the most popular services for entrepreneurs is the registration of sole proprietorships and limited liability companies on the Diia portal. This is the fastest business registration in the world. In 10 minutes, with a digital passport and a signature in Diia, you can become an entrepreneur - open a sole proprietorship without leaving your home.
The war posed new challenges, so the priorities of the Ministry of Digital Affairs have changed. In the first weeks after the full-scale invasion, e-Document was launched – a unique document for the time of martial law that contains passport data and an identification code. Diia is also a comprehensive service for internally displaced people, and it is one of the most relevant services. 1.4 million people have applied for certificates and cash assistance for IDPs through Diia. The chatbot e-Vorog has become a powerful tool of public intelligence. You can file a claim for the damaged property through Diia. They also launched the e-Oselya

affordable lending program. Military bonds in Diia became another essential tool for supporting the country's army and economy.

One of the most used services is e-Malyatko, a comprehensive service for newborn parents. With one application submitted online, you can register a child's birth and receive up to 10 public services from various authorities that are required at the time of the birth.

Digitised diplomas became one of the latest innovations in Diia. You can enter a higher education institution or get a job without many photocopies - it is enough to share an electronic educational document.

One of the updates in 2024 was the Marriage online service – distance will no longer hinder love. Even if «*the other half*» is thousands of kilometres away, you can propose and get married in Diia. To propose marriage, click the «*Propose*» button. Your loved one will receive a notification with the offer and have 14 days to decide. Diia also has a marriage certificate.

In addition, in September 2024, a new function was launched in Diia - e-Residence. This is an online service that enables foreigners to conduct business online in Ukraine and open bank accounts. The service allows e-residents to share their business without the need for a physical presence in Ukraine. Services for IDPs, damaged property, payments from the state, and unemployment benefits were also implemented.

An essential component of the digital state is the Trembita system, thanks to which registers exchange data. This is an analogue of the Estonian product X-Road, which was adopted in Ukraine. Diia does not store personal data. The application was created in 2019, and it was already during the war. It was analysed, and possible cyberattacks and threats were predicted. Therefore, I approached the Diia architecture, taking into account all potential risks. And now, we can say that it was built perfectly for wartime.

The Minister of Digital Transformation noted, «*The safety of Diia users is our top priority. Twice, we conducted the Bug Bounty program, in which ethical hackers tested the application and searched for vulnerabilities for a reward of 1 million hryvnias. These were Diia crash tests that did not reveal any critical vulnerabilities*».

Diia is a structured process that involves simple interaction and convenience. An application that helps every person. Ukrainians are proud of Diia, talk about it

abroad, and teach their grandmothers to use the application. Stand-up comedians joke about Diia, make tik-toks, and discuss her on Twitter. If earlier the ministers were cautious about Diia, now they are thinking about how to make the service digital first and then take it offline. This is a complete change in the government's work philosophy. The most important result of the last years of work is creating a new technological culture in the state. Now, each service is designed according to the digital-first approach - first online, and only later, if necessary, does it appear offline.

Even despite the war, we were able to export our digital products. An analogue of our Diia will work in Estonia. In addition, according to our Minister of Digital Transformation, several European, Asian, and African countries are interested in the Ukrainian state application.

Gradually, Diia became a super-app – a single window of communication with the state, a universal application where you can get all government services. Ukrainians are already used to the fact that all the most popular services can be obtained in Diia, and they are waiting for the appearance of new services in the application, not offline. This is another confirmation that a faster and more convenient future awaits us. Even though Diia is a progressive step in the country's innovative development, this application is still not perfect.

It should be noted that the Diia application is not being used to its full capacity. Not all members can use it, as there are still some technical limitations and access barriers for specific user groups. In particular, previously, insufficient attention was paid to ensuring the application's accessibility for people with disabilities – vision, hearing, etc. Special functions and settings that will facilitate the work with Diia for such users must be implemented. In addition, the application's use is restricted to senior citizens or those with little knowledge of digital technologies. Special educational programs and materials must be developed to facilitate the work with Diia for such users.

So, after researching the current state of development of the Diia mobile application, we can conclude that Ukraine has become a pioneer in the legalisation of digital documents on par with plastic IDs. Corresponding changes were made to the legislation, in particular, the Law On the Unified State Demographic Register, which gave legal force to electronic documents certifying the identity of citizens. Thus, our state was the first in the world to equalise the

status of digital and plastic IDs and laid the legal foundation for further comprehensive digitisation of the field of personal identification and its special status.

The problems faced by public administration in the field of digital transformation under martial law are not an obstacle to the development of digitalisation in Ukraine but rather a driving force. In military conflict, the state actively intensifies dialogue with the public online to solve urgent problems effectively. Therefore, performance evaluation and further development of the Diia portal can, without objection, contribute to improving citizens' quality of life and optimising state management in such conditions.

4. Kyiv Digital – the city in the pocket

Kyiv has identified digital transformation as one of its central priority policies. In recent years, Ukraine has been growing in awareness and recognition of digital transformation as a key factor in the future development of its economy. Among the most significant achievements in the digital development of Ukraine, experts note the following: creation of the Ministry of Digital Transformation of Ukraine; the launch of the portal of public services and mobile application Diia; expansion of the range of electronic public services; development of the field of electronic communications and improvement of the system of providing online electronic trust services; increasing the number of initiatives in digital education; development of a strategy (roadmap) for the integration of Ukraine into the Single Digital Market of the European Union[52].

Legislation on the digital economy and telecommunications, the availability of digital infrastructure, and achievements in the cashless economy, in particular, the development of electronic trade (e-Trade), electronic protection (e-Trust), and cyber security (Cyber-security), are prerequisites for the continued growth of digitalisation. Also, the top changes started with the smart city, which was implemented through electronic doctor's records, open budgets, and a transparent city, where we open up all procurement data. Everyone, not only a citizen of the city but also a citizen of Ukraine from other cities, can come in and see how budget funds are used, how work is carried out, on which streets, what is being done, etc.

The second thing is the activity of citizens in practical changes in the city. If there had been protests and pickets earlier, people would have started to take an active part in the life of the city. They are involved in the public budget and use it as they see fit. The townspeople consolidate among themselves and form working groups. Someone is engaged in the preservation of architectural heritage, someone is involved in eco-projects, and someone is engaged in the arrangement of urban space: benches, parks, and lighting. This is the biggest, in my opinion, success! Electronic self-government contributed to the emergence of "smart citizens". These are people who learn to think and know how to use the opportunities and resources they currently have. Because many people do not know that they can influence the positive development of the city through their efforts, you can not waste your time, but you can solve cases through electronic services.

Implementing the concept of a smart city is no longer unusual for citizens, but you should not think that Ukraine stands aside from innovative changes. According to the World Ranking Smart City Index 2021, Kyiv rose 16 points and took 82nd place, which is only one of the best growth dynamics[53].

Smart City is a city initiative founded in 2015 with the aim of technologisation of the capital of Ukraine, the city of Kyiv, through the implementation of the Kyivcard projects, online records and support of city projects with the introduction of an open data portal, online doctor appointments, electronic queues for kindergartens, a comprehensive system video surveillance, electronic petition systems, etc. The project aims to technologicalise the Ukrainian capital, Kyiv, and implement and support city projects within the framework of the "Kyiv Smart City 2020 Concept". In the future, Kyiv will use "Kyiv Smart City" as a general development concept, based on which other strategies are approved. Currently, Kyiv has a city development strategy until 2025[54].

The "Kyiv Smart City" application was later transformed into the pride of the capital – "Kyiv Digital", which started working in 2021. Today, the city application is the best assistant for Kyiv residents, allowing you to quickly purchase a ticket for city transport and find the nearest bus stop or the address of a car parking lot. Creating a capital application is a unique and original service for the city of Kyiv and Ukraine in general. In the first two years of operation, "Kyiv Digital" received its first million users. Due to the full-scale intrusion, several

functions were added to the application: blackout schedules and information about the radiation background in the capital. The capital plans to make "Kyiv Digital" the primary communication tool of city services with citizens.

"Kyiv Digital" cooperates with municipal parking lots. You can pay for hourly parking or purchase a parking pass from your smartphone, top up a transport card, buy a monthly pass, and use one-time QR tickets. The configured notification system will remind you when the travel card expires or tell you when the QR ticket expires. Also, if the user adds the residential address, "Kyiv Digital" will notify the user about the beginning and end of planned or emergency restoration work in the building. The application will give you notifications about electricity, water, gas, and heating services.

The "smart environment" category is, unfortunately, poorly developed in Kyiv. Because many factors in the city significantly affect the ecology and health of the population. Also, the use of technologies of alternative energy sources is slowly developing here. However, for the first time, Kyiv was included in the international rating "Global Cities: new priorities for the new world" 2020 Global Cities Report in the publications "Global City Forecast" (GCO) and "Global City Index" (GCI). The capital is 94th and 89th out of 151 cities in the world[55]. Thus, developing Kyiv as a smart city allows for solving the main challenges and making it more comfortable and safe for life. Implementation of this mission is possible due to modernisation and innovation, digital transformation, the implementation of energy efficiency principles, and the use of technologies of alternative energy sources that reduce the negative impact on the environment.

The creation of Kyiv's smart infrastructure began nine years ago. Today, Kyiv can share with other cities its experience of implementing successful innovative solutions that make residents' lives safe and comfortable and city management processes open and transparent. A virtual mayor, digitisation of trees, historical monuments, and mental health programs for those affected by the war - this is not a list of all the online services that are currently available in Kyiv.

From the first days of the Russian-Ukrainian war, it became clear that anyone could suffer from airstrikes and missile attacks. Against this understanding came the realisation that despite the common threat, not everyone had access to hazard warning systems. People could not hear sirens, did not have access to official

messengers of territorial communities, and did not know what to expect from the enemy.

The Air Alarm application was created to provide additional information about the situation in different regions of the country. This unique case became an alternative to the outdated street notification system. The main idea of the future product was to support critical notifications. This means that messages are received even when the smartphone is in silent or do-not-disturb mode[56]. The air alert is triggered when the radar systems of the Air Force of the Armed Forces of Ukraine detect the movement of enemy aircraft toward Ukraine's territory. A siren indicates that an aircraft that can attack with bombs or missiles is approaching a specific region or that a rocket has already been launched. Alerts are accompanied by a sound signal, which is different from other messages. This allows you to react quickly to danger and immediately go to the shelter. After each revocation of the air alarm, "Kyiv Digital" reports how long the threat lasted in the city.

Another function that I would like to pay attention to is news. It varies depending on the time. These can be warnings about street closures or events taking place in the capital. This information can be helpful for city drivers who use their transport or ordinary citizens who want to come to celebrate a particular event.

The last features I will look at are Petitions and Polls. This is an incredible opportunity for Ukrainians to contribute to changes in the capital. You can leave and confirm your vote directly in the application, which allows most people to do it quickly and conveniently.

Kyiv has also made great strides in implementing the Safe City concept, which is implemented through video surveillance cameras. In addition, residents of the capital have access to information about the budget and electronic procurement systems. There is also an option to fill out petitions and an opportunity to observe the map of emergency works.

Despite the hostilities, in November 2022, Kyiv presented innovative city projects at the Smart City Expo congress held in Barcelona. At the congress, Kyiv presented the city application "Kyiv Digital" and talked about introducing digital services in the Ukrainian capital. Our capital competed on the same level with Seoul (South Korea), Toronto (Canada), Sydney (Australia), Bogotá (Colombia),

and Curitiba (Brazil). The Head of Digital Transformation of Kyiv and the Deputy Head of KMDA emphasised, «*Participation in one of the largest technological events is an opportunity to declare yourself to the whole world. We want everyone to know Kyiv as a digital capital*»[57]. According to the results of the congress, the honorary jury decided to award Kyiv with a special award of the city for strengthening the stability and continuity of providing services to citizens. Withstanding the increasing pressure of the Russian siege, the Kyiv Municipal Authority demonstrates how digital technologies help cities stay resilient with a focus on public safety and a sustainable, multimodal mobility system while ensuring 100% of administrative services online by 2030[58]. It is a global community dedicated to establishing and advancing global policy norms for the responsible and ethical use of smart city technologies.

Kyiv also became a member of the G20 Smart Cities Alliance in 2023. The G20 Global Smart Cities Alliance is a global community of world leaders in the field of digital transformation. It's nice that Kyiv is now officially one of them[59]. Thanks to this, Kyiv will have access to experience, best practices, and tools developed by G20 participants. Our unique knowledge of ultra-fast digitisation in wartime will be helpful in many European cities.

5. Other digital services

The digitisation of our state globally started more than four years ago. The goal is to optimise processes, make them transparent and convenient for citizens, and minimise bureaucratic red tape. Queues, receptions, records, and "arrangements" are not required for help. You can get it here and now on your smartphone because the state is also a service.

In 2021, the mayor of Kyiv can be seen in the Brama augmented reality application. Virtual Klitschko appears on Volodymyr Hill and Natalka Park. The head of the city can also be seen at Sikorsky Kyiv Airport. The Brama application was developed exclusively for augmented reality. Also, starting in 2021, the digitisation of trees will continue in Kyiv. It is known that the city has more than 107,000 green spaces. The director of the Department of Environmental Protection and Adaptation to Climate Change said, «We *had two goals in creating this resource. First, a clear inventory must be conducted to understand how*

many trees there are in the capital and in what condition they are. Secondly, to provide the community with effective control tools. The online map is being filled»[60].

During the war, questions regarding quick access to public services that could be used remotely became even more urgent. Health is a prominent issue. This is precisely why the Helsi application works in Ukraine. In 2016, a health care reform was launched in our country, which provided for the creation of an information and telecommunications system for automating the accounting of medical services and managing medical information called Helsi. It was recognised as one of the most promising in the world. Helsi is about electronic prescriptions for medicinal products, the formation and closing of a sick leave certificate without visiting a doctor, consultations with more than 19 thousand doctors, and 17.2 million concluded declarations with doctors. At the same time, an information site for patients helps. I was created, with the help of which citizens can choose a family doctor, sign a declaration for the provision of services with him, make an appointment for vaccination or a doctor's appointment at a time convenient for them, and monitor their medical card and doctor's appointments online[61].

Also, there is an electronic queue for enrollment in kindergartens in Ukraine. Due to the lack of places in kindergartens, you can join the electronic queue immediately after the birth of a child. The earlier you join the queue, the greater your chances of getting a place in the selected kindergarten are. You can authorise or create your Kyiv ID account, fill in an application form and choose kindergartens to register your child. For this, you can use the Parent's office.

Digitisation of cultural heritage objects will expand the possibilities of developing the capital's tourism potential. For example, thanks to the preserved digital data, Notre Dame Cathedral was restored after a fire in the spring of 2019. Based on these data, various issues were solved, from large construction tasks to interior decoration with small elements. «*We will have digital copies – three-dimensional models of objects of our monuments. In wartime, when the enemy destroys civilian infrastructure, monuments of our history and architecture often come under fire. Such cooperation will help us, at least, not to lose the destroyed*» emphasises the Director of the Department of Cultural Heritage Protection of the KMDA[62].

The most successful cases of capital are the video surveillance system, the

platform of registers and services, which made it possible to create a resident's office and a mobile application, as well as a public budget. In Kyiv, the most accurate and transparent service, Open Budget, has been developed, where data is automatically uploaded to the system daily, and analysis by levels, administrators, purpose, etc., is available.

During the war, the Reserve+ application appeared – an electronic office where information about the status of conscripts and reservists could be obtained. The updated Reserve+ plan adds the possibility of registering three types of deferrals online: for parents of large families, people with disabilities, and full-time students. There should also be an online recruiting function with the ability to sign a contract or mobilise «*in two clicks*»[63].

On February 16, 2024, the Bloomberg Philanthropies charity announced exceptional support for Kyiv, which will accelerate digitalisation in the field of mental health. «*Kyiv, even under martial law, continues to develop digital services for its citizens. In particular, this concerns the digitisation of services that meet the urgent needs of the capital's residents in the field of mental health and city sustainability. Thanks to the support of Bloomberg Philanthropies, Kyiv will become an even more comfortable and safer city with a more efficient city management system*» said Vitalii Klitschko[64].

6. Challenges and prospects

On the way to the digitalisation of state services, Ukraine overcame a problematic path and took several measures, including:

- reformed the field of electronic communications and harmonised the legislation of this area with the EU legislation;
- ensured compliance of digital identification and provision of trust services with national, European and international standards;
- the status of European qualified providers of electronic trust services is recognised in the country;
- we are working on introducing the paperless regime; implemented the reform of obtaining public services online, created fundamental rules for the operation of public electronic registers;

- impetus for the development of the IT industry. It is about the Diia-City concept, which is designed to strengthen Ukraine's competitive position;
- created a legal framework for the legalisation of the new market of virtual assets and the development of this business;
- legislatively introduced the principle of Cloud First, *i.e.* transfer of the main processes of production of IT servers to platforms of information and communication technologies based on cloud computing in the sphere of public administration, education, science and other spheres of public life;
- established organisational principles for the use of domain names in the unique public domain gov.ua by state authorities, local self-government bodies and state-owned enterprises, institutions, and organisations.

Although some of the services envisaged by the concept of smart cities are already operating in Ukraine, in particular, digital tickets for public transport, video surveillance systems on the streets and in the subway, electronic document management, online registration in hospitals and state institutions, etc., the general trend does not yet have an all-Ukrainian character.

The first problem Ukrainian cities face on the way to smart development is the lack of a strategic vision. For the successful implementation of this concept, Smart solutions must be officially enshrined in the development strategies of each settlement. Most megacities in developed countries follow this path.

The second problem is the lack of funding because the implementation of this concept depends not only on the government but also on business investments. That is, smart cities technically cannot appear only with budget funds. Today, businesses, investors, and patrons do not actively participate in the development and implementation of the Smart concept.

The third problem in Ukraine is the lack of qualified and experienced personnel who can launch and support innovative solutions. We are talking not only about actual workers who can implement the global smart experience in Ukraine but also about the only state body that would regulate these issues. After all, today, ministries, representatives of municipal authorities, non-governmental organisations and individual experts are working on the creation of smart cities.

Unfortunately, in modern Ukraine, the war has become the main pusher of

progress, particularly technical progress. Although our national struggle has been going on for more than a century, it was the full-scale invasion of a neighbouring state that became a sufficiently robust post to unite Ukrainians both within the country and abroad. Since the beginning of Russia's war against Ukraine, not only has the government gone into martial law, but the apps have also enabled new notifications and added new features to meet today's challenges. New mobile applications can be helpful to Ukrainians in the conditions of martial law and solve the problems of communication between citizens and the state, particularly for quickly obtaining systematised and verified information. The capital is faced with the task of a safe urban transport system, including the introduction of automated roads, autonomous cars and means of travel. Also, restoring the medical system, providing it with the latest IT and modern medical equipment, and attracting and training highly qualified specialists.

Reducing the level of pollution and water consumption, using infrastructure for resource efficiency, and its reverse use in a closed-loop system. Creation of innovative platforms for managing waste flows based on its reuse and environmentally safe recycling. At the same time, traffic jams, air pollution and affordable housing are issues that concern citizens. Loss of information on outdated devices, the danger of malicious use of personal information, misinformation, and misuse of artificial intelligence are the main threats of digitalisation, and capital authorities face such tasks. There is also a danger of social inequality because a significant percentage of the population does not have access to the Internet and, accordingly, the appropriate levers of influence to use the benefits of digitalisation.

It is important to mention that, in Ukraine, both at the central level and at the local level, several regulatory legal acts have been adopted for the implementation of Smart City, in particular, the Law of Ukraine "On the Protection of Personal Data", the Law of Ukraine "On the National Informatisation Program", the Law of Ukraine "On Local Self-Government in Ukraine", the Law of Ukraine "On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015", The Sustainable Development Strategy "Ukraine-2020", "The Concept of the Development of the Digital Economy and Society of Ukraine for 2018-2020", the Decision of the Kyiv City Council "On Approval of the Concept «Kyiv Smart City 2020»" and the Decision of the Lviv City Council

"On Approval of the Digital Transformation Program of Lviv for 2016-2020".
Although these normative legal acts have either expired and had a limited period of implementation or they provide general information on the settlement of the Smart City concept, the Law in Ukraine has not yet regulated it. The declarative nature of these acts did not allow for the implementation of the relevant measures outlined by them into a practical plane.
Currently, Ukraine has a Concept for developing digital competencies until 2025[65], which has a significant influence on the development of the state within the context of Ukraine's implementation of the Association Agreement with the European Union. The Agreement provides for the adaptation of Ukrainian legislation to EU legislation. In turn, the EU introduced the so-called "E-Regulator of Digital Competencies for EU Citizens", which helps individuals to assess their knowledge in the digital sphere or identify gaps in their skills. Thus, with the help of the Concept, Ukraine harmonizes the national digital market with the EU countries.
The Law of Ukraine "On Local Self-Government in Ukraine" does not contain norms that would directly determine the powers of local self-government bodies to introduce the concept of a smart city in practice. Indeed, outlining the powers of local governments to develop the city based on reasonableness will allow for a more active implementation of the Smart City concept, which will be especially important in connection with the tasks of post-war restoration of the country's settlements. At the same time, in modern conditions, it is possible to rely on the general provisions of this Law because the essence of local self-government following Part 1 of Art. 2 of the Law[66] lies in the ability of local self-government bodies to independently resolve issues of local importance within the framework of the Constitution and laws of Ukraine.
The Decree of the President of Ukraine "On the Sustainable Development Goals of Ukraine for the period up to 2030"[67], defined the task of sustainable development of cities and other settlements. The development of a city based on sustainability can ensure the implementation of the concept of Smart City, which actualizes the task of practical implementation of this concept.
Despite all the challenges of a full-scale war, Ukraine is moving towards the European Union. We are aware that our future, our values and our development are there. Our task includes harmonising legislation with European legislation in

the field of digitalisation. The adoption of a long-term strategy of digital transformation and digitisation corresponds to the processes of European integration, increases the level of public trust between state authorities, local self-government bodies, and the population of the country or territorial communities, and promotes transparent communication and flexibility of the service delivery system.
And here I have a proposal:

- unify the legislative framework – the development of digitalisation of public services should be based on a clear legislative framework, in particular by adopting the Law on Smart City and the same time, Ukraine needs to implement the Recommendations of the Council of Europe on electronic voting on the way to its European integration;
- achieving public consensus – for the introduction of new electronic services in the field of public administration, it is necessary to reach a broad public consensus, especially among key political actors. This will contribute to the strengthening of trust in the new type of service; ensuring technological development - before the introduction of new electronic services, it is essential to ensure extensive preparation for this process through the development of technologies and citizens' computer literacy. State policy in the field of technological development and education should support the wide use of digital technologies by the population and ensure their reliability; to create at the national level a unified platform for the exchange of experience between the cities of the country;
- carry out information and educational campaigns and provide access to high-speed Internet throughout Ukraine – before the introduction of new electronic services, it is necessary to conduct an explanatory campaign to inform citizens about the advantages associated with the use of these services;
- apply a scientific approach to the digitization of public services. This should be thoroughly researched using scientific methods. This will not only contribute to their improvement but also strengthen citizens' trust in digital tools in democratic processes.

These recommendations can contribute to improving the digitalisation processes of public services in Ukraine in the context of democratic development of society, ensuring their transparency, public trust, and efficiency. In turn, this will provide an opportunity to ensure the development of the Ukrainian state on a democratic basis.

In today's realities, the presence of a Smart concept is a strategic necessity. And no matter how unfortunate it sounds, the war can provide a reasonable basis for the development of the system of smart cities in Ukraine. That is, the country has the opportunity not only to restore destroyed towns but also to build them in a new way, taking into account modern trends and world experience. In addition, in the future, this concept will not only make Ukraine more innovative, competitive, and attractive to Ukrainians and foreign citizens. Still, it will also attract a significantly more significant number of investors to the development of the state.

7. Conclusions

The concept of a Smart City provides municipal authorities access to large volumes of data, which simplifies the solution of many problems but also requires officials to make decisions solely based on the full availability of data. However complex the process of implementing change may be, it ultimately makes life in cities safer and more convenient. In general, three central components connect the state and the citizens and allow them to interact at a distance. These are data exchange between registers, the ability to identify citizens, and equal access to digital services. The digital state is about the exchange of data between registries. Data should run, not people. Each state body, with the consent of a person, must collect data from the state register. The more exchanges we customise and change these processes, the more unnecessary services and help disappear.

The issue of digitalisation of the system of administrative services is currently critical, especially in the conditions of martial law, and requires the development and adoption of a long-term strategy of digital transformation and digitalisation. According to N. Khliborob's definition, «*Digitalisation is not about technology, but about the people for whose benefit these technologies should serve. Emphasis*

should be placed not on the number of services but on how accessible, convenient and useful they are for people. The focus should be on the observance of fundamental human rights in the conditions of digitalisation, and digital technologies should be applied based on guaranteeing these rights»[68].

That is, Ukraine is about a digital signature, digital services, comfort and speed for business, and a minimum of paperwork and red tape. But we are aware that we still have a lot to work on. In addition, our goal is not just to integrate into the EU but to integrate in such a way that we bring as much benefit to the community as possible, not the threats many fear. The development of the smart city in Kyiv began in 2015. During this period, the city authorities managed to implement several important projects for the transformation of the urban environment. However, it is worth noting that this development is relatively slow, and decisions are often made without taking into account the needs of the citizens – the risk of corruption, lack of political will and lack of funding.

Also, improving the system of local self-government based on the use opportunities provided by the development of digital technologies is an important component in overcoming the devastating consequences of the Russian Federation's military aggression against Ukraine and ensuring post-war recovery. Implementing smart city technologies can also be an important component of this process.

The concept of a smart city involves using communication and information technologies to develop better management strategies and make important decisions. Transforming a city into a smart city is a long-term process that requires large resources and funding. Cities must first choose those areas for transformation where modernisation and the application of digital technologies are most necessary. In particular, the world experience of smart cities shows the importance of an individual approach to the development of this concept.

The war with Russia affected all spheres of life and industry in Ukraine, including the mobile application market. All the aforementioned applications and their newly created functions demonstrate the desire to help loved ones, the most human desire in society, which seeps even into smartphones. Perhaps, after the victory of Ukraine, all these applications and their "military functionality" will disappear from our devices. Still, now we can read the national thirst to fight for our freedom and independence behind the icons on the screen.

1. 1 This article was written under the umbrella of the 4 EU+ *Chartering the course towards a legal framework for smart cities* (reg. č. MA/4EU+/2024/F3/04).
2. Y. Tretyak, *Industries of the future: «smart» cities and houses,* in *online magazine «Mind»*, 2018, https://mind.ua/publications/20188390-galuzi-majbutnogo-rozumni-mista-ta-budinki.
3. *Country profiles on housing and land management, Ukraine,* in the official website of the United Nations Economic Commission for Europe, https://unece.org/DAM/hlm/documents/Publications/CP_Ukraine_ECE.HPB.176.en.pdf.
4. T. Dixon, *Smart and sustainable?: The future of the «future bridge»,* in T. Dixon, D. Connaughton, S. Green (Eds.), *Sustainable futures in the built environment to 2050: A foresight approach to construction and development*, Oxford: Wiley-Blackwell, 2018, pp. 94-116.
5. D. Washburn, *Defining the Smart City, Its Drivers, and the Role of the CIO*, in D. Washburn, U. Sindhu, S. Balaouras, R.A. Dines, N.M. Hayes, L.E. Nelson, *Helping CIOs Understand «Smart City» Initiatives*, Cambridge, in *MA: Forrester Research, Inc.*, 2010, https://www.forrester.com/report/Helping-CIOs-Understand-SmartCity-Initiatives/RES55590.
6. B. Cohen, *The Smart Cities in the World: Methodology*, in *online magazine Fast company*, 2014, https://www.fastcompany.com/3038818/the-smartest-cities-in-the-world-2015-methodology.
7. R. Giffinger, H. Gudrun, *Smart cities ranking: An effective instrument for the positioning of the cities?*, in *Architecture, City and Environment,* 2010, No. 4 (12), pp. 7-26, https://core.ac.uk/download/pdf/301204045.pdf.
8. P. L. Lombardi, *The Challenge of Designing User-Centric e-Services: European Dimensions*, in P. L. Lombardi, I. Cooper, K. Paskaleva, M. Deakin, S*trategies for Local e-Government Adoption and Implementation: Comparative Studies,* Hershey: Idea Group Publishing, 2009, pp. 460-477.
9. A. Murray, M. Minevich, A. Abdoullaev, *Being Smart and Smart Cities,* in *The Future of the Future*, 2011, pp. 20-23, https://www.kmworld.com/Articles/Columns/The-Future-of-the-Future/The-Future-of-the-Future-Being-smart-about-smart-cities-77848.aspx.
10. V. Albino, U. Berardi, R.M. Dangelico, *Smart cities: Definitions, dimensions, performance, and initiatives,* in *Journal of Urban Technology*, 2015, 22(1), pp. 3-21, https://www.tandfonline.com/doi/full/10.1080/10630732.2014.942092.
11. J. Handrlica, *Introductory Note to «Regulatory Sandboxes, Automatization of Administrative Decision-Making and the Future of Administrative Law»,* in *Acta Universitatis Carolinae Iuridica*, 2024, No. 70 (2), pp. 9-11, https://www.ceeol.com/search/article-detail?id=1242584.
12. M. Bernardo, *Smart city governance: From e-government to smart governance*, in *Smart*

cities and smart spaces: Concepts, methodologies, tools, and applications, edited by I*nformation Resources Management Association*, IGI Global, 2019, pp. 196-232, https://www.igi-global.com/chapter/smart-city-governance/211292.

13. A. Camero, E. Alba, *Smart city and information technology: A review*, in *Cities,* 2019, No. 93, pp. 84-94, https://smartcitycluster.org/wp-content/uploads/2021/03/smart-city-and-it-review-2019.pdf.
14. J. Chen, Y. Guo, C. Su, J. Chen, S. Chang, *A smart city system architecture based on a city-level data exchange platform,* in *Journal of Information Technology Research,* 2015, No. 8(4), pp. 1-25, https://www.igi-global.com/article/a-smart-city-system-architecture-based-on-city-level-data-exchange-platform/145391.
15. M.J.N. Han, M.J. Kim, *A critical review of the smart city in relation to citizen adoption towards sustainable smart living*, in *Habitat International,* 2021, No. 108, Article 102312, https://www.researchgate.net/publication/348689328_A_critical_review_of_the_smart_city_in_relation_to_citizen_adoption_towards_sustainable_smart_living.
16. B. N. Silva, M. Khan, K. Han, *Towards sustainable smart cities: A review of trends architecture components and open challenges in smart cities,* in *Sustainable Cities and Society,* 2018, No. 38, pp. 697-713, https://www.researchgate.net/publication/323511300_Towards_sustainable_smart_cities_A_review_of_trends_architectures_components_and_open_challenges_in_smart_cities.
17. Yu. Danko, N. Bilotserkivska, *Electronic voting: possibilities of Ukrainian reception,* in *Modern society: political sciences, sociological sciences, cultural sciences,* 2019, vol. 1, No. 17, pp. 60-72.
18. L. Marchenko, *Digitization of the tax administration system in Ukraine taking into account the experience of the developed countries of the world,* in *Economic Analysis,* 2022, vol. 32, No. 4, https://www.econa.org.ua/index.php/econa/article/view/2933.
19. G. Ortina, N. Rybalchenko, *Digitization of public authorities,* in *Public Administration,* 2022, No. 1 (29), pp. 104-109, http://repositsc.nuczu.edu.ua/bitstream/123456789/13274/1/OrtinaRybalchenko.pdf.
20. M. Polishko, *Digitization of management processes: world experience,* in *Public management and administration: materials of the 78th Student Scientific and Technical Conference «Student Science Week»*, 2023, pp. 592-593, http://ir.nmu.org.ua/handle/123456789/164354.
21. O. Stogova, D. Murach, *Electronic voting: problems and prospects of implementation*, in *Juridical scientific and electronic journal,* 2021, No. 3, pp. 38-41, https://www.researchgate.net/publication/367948625_ELECTRONIC_VOTING_PROBLEMS_AND_PROSPECTS_OF_IMPLEMENTATION.
22. R. Frosinyak, *Peculiarities of implementation of digitization of participation in elections as a global trend,* in *Bulletin of the NUTSZ of Ukraine, Series: Public Administration, 2022,*

vol. 2(17), pp. 139-148, https://www.researchgate.net/publication/376869291_Zarubiznij_dosvid_vprovadzenna_elektronnogo_golosuvanna_organizacijni_ta_pravovi_aspekti.

23. I. Zhukovich, *Smart cities as a new object of statistical research: definition of the term,* in *Statistics of Ukraine*, 2015, No. 1, pp. 18-22.
24. S. Chukut, V. Dmytrenko, *Smart city or electronic city: modern approaches to understanding the implementation of e-government at the local level*, in *Investments: practice and experience,* 2016, No. 13, pp. 89-93, http://www.investplan.com.ua/pdf/13_2016/17.pdf.
25. T. Pushkar, D. Serogina, K. Mykhailova, H. Zhovtyak, H. Sobolieva, *World Experience of Smart City Development,* In O. Arsenyeva, T. Romanova, M. Sukhonos, Y. Tsegelnyk, (eds), *Smart Technologies in Urban Engineering*, STUE 2022, Lecture Notes in Networks and Systems, vol. 536, in *Springer*, Cham, https://link.springer.com/chapter/10.1007/978-3-031-20141-7_55.
26. T. Pushkar, *Dyzain-myslennia v realizatsii innovatsii staloho rozvytku mist [Design thinking in the implementation of innovations in the sustainable development of cities], Sustainable development of the national economy: current problems and security mechanisms: materials of the International scientific and practical Internet conferences,27April 2023,* Kryvyi Rih, pp. 121-123.
27. I. Opirskyi, O. Tiutikov, *Problema pobudovy kontseptsii «Rozumnoho mista»* [*The problem of building the «Smart City» concept*], in *Ukrainskyi zhurnal doslidzhen informatsiinoi bezpeky [Ukrainian Journal of Information Security Research]*, 2020, vol. 22, No. 2, pp. 114-119.
28. O. Tur, *Kontseptsiia rozumnoho mista yak osnova zabezpechennia staloho rozvytky terytorii* [*The concept of a smart city as a basis for ensuring the sustainable development of territories*], in S*khidna Yevropa: ekonomika, biznes ta upravlinnia*, 2018, vol. 4 (15), pp. 286–289.
29. I. Antonyuk, S. Koshova, *Implementation of smart-city programs in large cities: domestic and foreign experience,* in I*nvestments: practice and experience,* 2021, No. 18., pp. 99-107.
30. V. Vorobyov, O. Shilo, *Features of the stylistic combination of old and new architecture in the conditions of the post-war reconstruction of Ukrainian cities,* in *Ukrainian Journal of Construction and Architecture*, 2022, No. 2.
31. L. Zhilinska, H. Kucherova, O. Tarasevich, *Application of the Smart-city concept to solving the tasks of restoration and development of spheres of urban life in the post-conflict territories of Ukraine,* in *Economy and law*, 2020, No. 4, pp. 51-58.
32. O. Zakharova, D. Kozyrev, *The concept of a smart city as an alternative approach to the restoration of the urban infrastructure of Ukraine in the post-war period,* in *Collection of scientific papers of the Cherkasy State University of Technology, Series: Economic sciences*, 2022, Issue 67, pp. 5-14.
33. T. Palamarchuk, *Impact of globalization processes on municipal transformations: development of Smart Cities,* in *Public administration: improvement and development,* 2024, No.1, http://doi.org/10.32702/2307-2156.2024.1.12.

34. O. Palyvoda, O. Bondarenko, *European approaches to the marketing of smart cities,* in *Efficient economy*, 2024, No. 1, https://doi.org/10.32702/23072105.2024.1.1.
35. N. Protsyuk, *Conceptual foundations of the interpretation of the essence of the Smart infrastructure of cities in the context of sustainable development,* in *Scientific innovations and advanced technologies*, 2024, No. 1(29), pp. 116 - 127.
36. K. Radchenko, *Modern foreign approaches to defining the concept of «smart city»,* in *Economic management: theory and practice*, 2022, No. 14, pp. 184 - 185.
37. N. Skorobogatova, *Implementation of the EU experience regarding the transition to the urban green economy as a model of the post-war reconstruction of Ukrainian cities,* in *Scientific Bulletin of the Uzhhorod National University. Series: International economic relations and world economy*, 2022, Issue 44, pp. 96-102.
38. M. Gramchuk, V. Nikitenko, *Present trends and prospects of smart city development,* in *Humanities studies*, 2023, Vol. 14, pp. 35-41.
39. I. Dunaev, N. Gavkalova, A. Kud, p. 38.
40. N. Komninos, *The Age of Intelligent Cities: Smart Environments and Innovation-for-all Strategies,* in *London: Taylor & Francis Group*, 2018, p. 298.
41. Singapore Government Portal, on the official website, https://www.gov.sg.
42. Digital Government, on the official website, https://www.canada.ca/en.html.
43. Government portal of Estonia, on the official website: https://www.eesti.ee/ru.
44. *Ibid*.
45. I. Antonyuk, S. Koshova, *Implementation of smart-city programs in large cities: domestic and foreign experience,* in *Investments: practice and experience*, 2021, No. 18, pp. 99-107.
46. Amsterdam Smart City, on the official website, https://amsterdamsmartcity.com.
47. M. Gramchuk, V. Nikitenko, p. 39.
48. *Smart city strategies. A Global Review 2017*, https://cp.catapult.org.uk/case-study/the-global-view-of-smart-city-strategies/.
49. *Smart and Connected City*, https://international.stockholm.se/governance/smart-and-connected-city.
50. V. Negoda, *Smart technologies are becoming a mandatory component of city and regional strategies of development,* in *Decentralization.ua*, 2019, https://decentralization.ua/news/10590.
51. M. Fedorov (Minister of Digital Transformation), *Diia for 3 years. How did Ukraine get a place in the world history of digitization?* in *online magazine «Economic Truth»*, 2023, https://www.epravda.com.ua/columns/2023/02/14/697034/.
52. Law of Ukraine No. 851-IV On electronic documents and electronic document circulation, 2003, https://zakon.rada.gov.ua/laws/show/851-15#Text.
53. *Kyyiv pidnyavsya na 16 punktiv ta uviyshov u top-100 rozumnykh mist svitu [Kyiv rose by 16 points and entered the top 100 smart cities in the world]*, 2021, on the official website of the city of Kyiv, https://kyivcity.gov.ua/news/kiv_pidnyavsya_na_16_punktiv_ta_uviyshov_u_top-100_rozumnikh_mist_svitu/.

54. *The Kyiv City development strategy until 2025 (new version),* on the official website of the Department of Economy and Investments of the KMDA, https://dei.kyivcity.gov.ua/content/strategiya-rozvytku-mista-kyieva-do-2025-roku-nova-redakciya1.html.
55. *For the first time, Kyiv entered the international ranking of Global Cities: new priorities for the New World,* on the official website of the city of Kyiv, 2021, https://kyivcity.gov.ua/news/kiv_upershe_potrapiv_do_mizhnarodnogo_reytingu_Global_cities_novi_prioriteti_dlya_novogo_svitu/.
56. M. Sparrow, *Ajax Systems Develops Warning App For Ukrainians In Just One Day,* in *Forbes*, 2022, https://www.forbes.com/sites/marksparrow/2022/03/02/ajax-systems-develops-warning-app-for-ukrainians-in-just-one-day/?sh=512680c25c3b.
57. P. Olenych (The head of the digital transformation of Kyiv and deputy head of the KMDA), *«Smart city»: Kyiv's innovative projects will be shown at the Smart City Expo congress in Barcelona,* in *online magazine «Public Kyiv»*, 2022, https://suspilne.media/kyiv/316128-rozumne-misto-innovacijni-proekti-kieva-pokazut-na-kongresi-smart-city-expo-v-barseloni/.
58. *World Smart City Awards - 2022 Winners*, on the official website of the Smart City Expo, https://www.smartcityexpo.com/2022-world-smart-city-awards/.
59. *Kyyiv stav chlenom al'yansu rozumnykh mist Velykoyi dvadtsyatky [Kyiv became a member of the G20 smart cities alliance],* on the official website of the city of Kyiv, 2023, https://kyivcity.gov.ua/news/kiv_stav_chlenom_alyansu_rozumnikh_mist_veliko_dvadtsyatki/.
60. O. Vozniy (Director of the Department of Environmental Protection and Adaptation to Climate Change), *Digitization of Kyiv: new projects and applications,* in *online magazine «Ty Kyiv»*, 2024, https://tykyiv.com/city/tsifrovizatsiia-kiieva/.
61. Helsi is a convenient medical information system, https://reform.helsi.me/.
62. M. Solovyova (Director of the Department of Cultural Heritage Protection of the KMDA), *Digitization of Kyiv: new projects and applications,* in *online magazine «Ty Kyiv»*, 2024, https://tykyiv.com/city/tsifrovizatsiia-kiieva/.
63. K. Chornogorenko (Deputy Minister of Defense for Digital Development, Digital Transformations and Digitalisation), *New useful functions will appear in the «Reserve+» application,* in *online magazine «Glavcom»*, 2024, https://glavcom.ua/country/society/u-zastosunku-rezerv-zjavljatsja-novi-korisni-funktsiji-1025681.html.
64. V. Klitschko (Mayor of Kyiv), *Digitization of Kyiv: new projects and applications,* in *online magazine «Ty Kyiv»*, 2024, https://tykyiv.com/city/tsifrovizatsiia-kiieva/.
65. No. 167-p/2001 (On approval of the Concept for the development of digital competencies and approval of the action plan for its implementation - Order of the Cabinet of Ministers of Ukraine), https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text.

66. No. 280/97-BP (The Law of Ukraine On Local Self-Government in Ukraine), https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.
67. No. 722/2019 (On the Sustainable Development Goals of Ukraine for the period up to 2030 - The Decree of the President of Ukraine), https://zakon.rada.gov.ua/laws/show/722/2019#Text.
68. N. Khliborob, *Reforming the sphere of administrative services,* on the official website of the Center for Political and Legal Reforms, 2023, https://pravo.org.ua/reformuvannya-sfery-nadannya-administratyvnyh-poslug/.

Smart Administrative Punishment: a Slippery Slope of Automated Decision-Making and its Economic Incentives in Public Law

Vladimír Sharp

DOI: 10.13130/2723-9195/2025-2-61

La crescente automazione delle sanzioni amministrative nelle città intelligenti segna un cambiamento radicale nell'applicazione della legge pubblica. Se da un lato il processo decisionale automatizzato migliora l'efficienza e la coerenza, dall'altro solleva preoccupazioni critiche circa i suoi reali incentivi e l'aderenza ai principi della sanzione amministrativa. Questo articolo esplora i meccanismi e il quadro legislativo che consentono una sanzione amministrativa intelligente, concentrandosi sull'applicazione del codice della strada e sugli incentivi fiscali che ne determinano la politica. Esamina criticamente i rischi di un'applicazione guidata dalle entrate, l'erosione delle tutele legali e la distorsione delle priorità amministrative. Analizzando casi d'uso come l'oggettivazione della responsabilità del proprietario del veicolo nella Repubblica Ceca, l'articolo mostra come l'automazione mal regolata possa compromettere principi legali come la proporzionalità, il giusto processo e la deterrenza. L'articolo sostiene che, sebbene l'efficienza sia un obiettivo legittimo, la razionalità economica non dovrebbe mettere in secondo piano la giustizia, richiedendo un approccio equilibrato che integri l'automazione con misure di salvaguardia contro gli abusi.

The increasing automation of administrative punishment within smart cities marks a transformative shift in public law enforcement. While automated decision-making enhances efficiency and consistency, it raises critical concerns about its true incentives and adherence to the principles of administrative punishment. This article explores the mechanisms and legislative frameworks enabling smart administrative punishment, focusing on traffic enforcement and the fiscal incentives that shape policy. It critically examines the risks of revenue-driven enforcement, erosion of legal safeguards, and distortion of administrative priorities. By analyzing cases such as the

objectivization of vehicle owner liability in the Czech Republic, the article shows how poorly regulated automation may compromise legal principles like proportionality, due process, and deterrence. It argues that while efficiency is a legitimate goal, economic rationality should not overshadow justice, calling for a balanced approach that integrates automation with safeguards against misuse.□

Summary: 1. Introduction.- 2. Administrative punishment and smart cities.- 3. Instruments of automation in current legislative framework.- 4. Incentives behind automated decision-making.- 5. Risks of economically incentivized administrative practices.- 6. Quo vadis, smart punishment?- 7. Possible solutions and considerations de lege ferenda.- 8. Conclusions.

1. Introduction

The rapid development of digital technologies has transformed urban governance, making smart cities one of the central testing grounds for innovative regulatory approaches[1]. Among various other "smart" regulatory tools, automated administrative punishment has gained prominence as a tool for ensuring compliance with public laws and regulations. While automated decision-making systems in the area of administrative offense prosecution and punishment have enabled public authorities to enforce administrative sanctions more efficiently, it also raises significant legal concerns that warrant closer examination.

Just like all fine things in this world, benefits brought by the automation of administrative punishment practices come at a cost. While the reasonableness and proportionality of that cost can be subject to a whole different debate extending well beyond the scope of this article, it is crucial to be conscious about the price being paid for efficiency and convenience, and make related decisions accordingly. Both policymakers and law enforcement should be aware of potential systemic risks and factor them in when introducing and deploying the innovative practices. In this particular case, such risks have to do with the intrinsic features of automated decision-making (or rather the lack thereof) and its rather obvious practical and economical aspects.

This article explores the implications of automated administrative punishment and critically examines the increasing reliance on automated administrative punishment within the framework of smart cities. By examining the existing use-cases of automated decision-making in sanctioning proceedings and investigating the fiscal incentives that partially drive the implementation of smart administrative practices, the author seeks to identify the risks associated with revenue-driven enforcement models and looks for a balanced approach that integrates economic rationality with principles of fairness, proportionality, and due process to ensure that automation serves as a tool for governance rather than a mechanism for financial gain.

By exploiting the doctrinal methodology in the form of a value-centered proportionality analysis and elements of a critical post-RIA assessment, the author puts some of the existing use-cases of automated administrative punishment to the test and assesses their effectiveness both in reaching the designated goals and protecting individual rights while doing so, subsequently identifying the associated risks. In the first part of the article, the author presents the concept of the so-called "smart administrative punishment" and reveals the relevancy of administrative offence investigation and prosecution in the context of smart cities. The author then explores individual tokens of automation in contemporary administrative law, presenting concrete use-cases on the example of Czech legislation. As the next step, the author explores the ways in which fiscal incentives shape the development of automated punishment practices. Last but not least, the article addresses the ultimate research problem regarding the extent to which economic incentives should be allowed to dictate the administrative practices and policymaking and individual risks arising from automation of administrative punishment, also critically assessing the effectiveness of the said systems and anticipating further development.

2. Administrative punishment and smart cities

As increasingly more cities all over the globe integrate digital technologies into urban governance, hence making the concept of smart cities a focal point for innovation in administrative enforcement and decision-making, it is no surprise that the area of administrative punishment (also known in different jurisdictions

as administrative sanctioning or administrative offences) did not remain untouched by this development. In fact, it was one of the first ones to deploy advanced technology and various types of quasi-automated or semi-automated systems to increase the efficiency of law enforcement, predominantly in urban areas, with the first prototypes dating back to 1960s and widespread implementation taking place from 1990s[2]. With the introduction of surveillance systems, automated monitoring, and AI-driven decision-making processes, it is hard to escape the reality of administrative punishment becoming increasingly automated.

Derived from the etymology of the term "smart cities", automated administrative sanctioning processes can be collectively (and somewhat ironically) referred to as "smart administrative punishment"[3]. This relatively general category may include various types of administrative practices depending on a specific jurisdiction, with the more court-centered punishment systems such as the United States using smart punishment features rather for e.g. tax fraud investigation and revenue collection (administrative punishment in the broader sense with sanctions in the form of tax penalties, fines and punitive interest)[4], and the systems based upon partial delegation of sanctioning to administrative authorities implementing automation into the investigation and prosecution of administrative offences and misdemeanors[5].

The most notable smart city initiatives have embraced automated enforcement mechanisms with varying degrees of legal and societal acceptance. One prominent example is automated traffic enforcement, where speed cameras, red-light cameras, and congestion charge systems use AI-powered image recognition to detect traffic violations and issue fines to registered vehicle owners[6]. Another common area of automation is tax compliance and fiscal monitoring. Many jurisdictions have implemented AI-driven tax enforcement mechanisms to detect underreporting and fraudulent activities. By cross-referencing financial transactions, property ownership records, and spending patterns, these smart city components aim to identify tax discrepancies for further investigation[7]. Environmental monitoring and enforcement have also seen increased automation, with cities deploying sensors and AI-based monitoring systems to regulate environmental compliance, including illegal waste disposal, air pollution violations, and excessive noise disturbances. Some of the more extreme examples

go even further and use automated social order enforcement has emerged in some smart cities through the deployment of facial recognition technology and predictive policing algorithms. AI-driven crowd analytics can detect unauthorized gatherings, while real-time surveillance may issue warnings or fines for minor infractions[8].

The shift to "smart-ification" of administrative punishment undoubtedly brings numerous advantages, such as enhanced efficiency, consistency of sanctioning, and resource optimization. For instance, studies show that the presence of speed cameras is effective in reducing the speed adopted by drivers, with this effect even partially generalizing to areas without cameras[9]. It is also reported that speed cameras seem to have an overall positive effect in terms of prevention of both traffic collisions in general[10] and traffic injuries and deaths[11]. However, the delegation of enforcement powers to algorithms also presents unique challenges, particularly concerning procedural fairness and its compliance with the constitutional principles governing administrative processes. Unlike traditional administrative processes that involve discretionary human judgment, automated administrative punishment operates within a rigid, pre-defined algorithmic framework, leaving little room for case-by-case consideration, but also creates new and quite unique problems so far unknown to the traditional doctrine of administrative law. While the issue of smart punishment raises many questions, such as cybersecurity of databases used for automated decision-making[12] or the so-called "black box" phenomenon[13], one of the less obvious problems has to do with the incentives (either direct or indirect) forming the autonomous decision-making or formed by such practice itself.

It is also necessary to mention the role of discretion in many enforcement systems, which constitutes a fundamental challenge in automating administrative punishment[14]. Administrative decision-making often involves case-specific evaluations, contextual considerations, and proportionality assessments, which are difficult to encode into rigid automated systems. Current artificial intelligence and machine learning technologies remain limited in their ability to replicate human judgment, particularly in scenarios where nuanced decision-making is required. Hence, the implementation of smart administrative punishment into the current regime tends to lead to either abandonment of discretionary considerations altogether, or to their generalization and

categorization, with both approaches coming with various downsides.

3. Instruments of automation in current legislative framework

The problems created by the current setup of smart administrative punishment are best demonstrated based on the example of an existing regulatory framework. The legislative frameworks governing automated administrative punishment vary across jurisdictions, but they generally incorporate key legal instruments that enable and regulate automation in enforcement. In order to explore and analyze the legislative tools enabling automated prosecution and punishment, it appears apt to narrow the scope of research down to a particular area of automation, with the most obvious choice being traffic enforcement, being one of the most widely recognized and well-documented applications of automated administrative punishment is traffic enforcement regulation.

Automated traffic enforcement mechanisms, such as speed cameras, red-light cameras, and congestion charge systems, have been in use for decades, providing a valuable case study for analyzing the broader implications of automation in administrative sanctions. This regulatory area serves as an ideal example for several reasons. First and foremost, traffic enforcement is inherently data-driven, relying on objective criteria such as vehicle speed, road positioning, and time stamps to determine violations. Unlike other domains of administrative punishment, where subjective factors or discretionary assessments may play a role, traffic enforcement lends itself well to automation due to its reliance on verifiable data points. This characteristic makes it an early adopter of automation, providing a wealth of case law, regulatory precedents, and empirical data to analyze. Secondly, traffic enforcement systems operate at the intersection of efficiency and fairness, embodying both the benefits and risks of automated administrative sanctions, which makes them a great specimen for testing the fragile balance between those conflicting interests. On the one hand, traffic enforcement systems reduce the need for human oversight, enabling authorities to process vast volumes of violations in a timely and cost-effective manner. On the other hand, they raise crucial questions regarding their compliance with the basic principles of fair prosecution, proportionality, and collateral problems

created by their use, which are issues that are central to the broader discussion on smart administrative punishment. Thirdly, traffic enforcement regulation can be considered one of the most globally standardized forms of automated punishment, making it relatively universal and relevant across different jurisdictions. While individual jurisdictions may vary in their approach to speed limits, fine structures, and procedural safeguards, the fundamental principles governing traffic enforcement are relatively consistent. And finally, the study of automated traffic enforcement provides insight into economic incentives driving automation in public law.

When contemplating possible models of traffic enforcement automation, several solutions corresponding to different levels of automation come into consideration, ranging from partial automation and detect-and-notify systems, through hybrid models incorporating human oversight, all the way to fully automated systems. In case of full automation, detection, violation assessment, and fine issuance can occur entirely without human intervention. This is the case with speed and red-light cameras that automatically capture violations and impose fines by means of full-fledged and binding administrative decisions based on pre-set legal thresholds[15]. Semi-automated and hybrid models incorporate an initial automated detection phase followed by human verification before sanctions are imposed. This model attempts to balance efficiency with fairness by ensuring that detected violations undergo a review process to filter out potential errors or misinterpretations. For example, some jurisdictions may require law enforcement officers to manually confirm that a detected violation, such as running a red light, meets legal standards before a fine is issued[16].

It is probably needless to emphasize that current regulatory frameworks in most jurisdictions were architected without automation in mind. In practice, that means that upon their initial deployment, smart administrative punishment practices had to play the hand it was dealt and make use of the existing legislation. A rather fascinating and relatively unique token of legal engineering can be found in Czech traffic legislation, which addressed the systematic inefficiency (caused by the combination of relatively strict burden of proof, understaffing of qualified personnel, and in many cases impossibility to identify the offender) by escaping the ordinary procedural regime and introducing a new concept sometimes referred to as “legal indulgences”[17]. This administrative practice, legalized by Sec.

125h of the Czech Road Traffic Act[18], allows authorities to forego formal prosecution of a traffic offense in exchange for a monetary payment by the vehicle owner[19]:

«*The administrative authority of the municipality shall, without undue delay after the discovery or notification of the traffic offence, invite the owner of the vehicle with which the offence was committed to pay a specified sum (...). Should the specified sum be paid not later than the due date, the administrative authority of the municipality shall defer the case. Otherwise, the administrative authority shall proceed to investigate and prosecute the offence*»[20].

Unlike standard administrative proceedings, where a formal charge is issued and contested, legal indulgences effectively work as take-it-or-leave-it plea deals. The recipient of such an offer may either choose to pay the specified amount, thereby avoiding potential prosecution and dodging the associated legal costs, or decline the offer and risk facing formal charges while not being protected by the *reformatio in peius* principle[21]. This mechanism operates outside the procedural framework of administrative proceedings, meaning that the notification issued by the authority does not constitute a formal administrative decision.

Although not designed specifically for the purposes of automated decision-making, this legal instrument can be (and is) exploited for the implementation of smart city ecosystems. Even though this system increases administrative efficiency, reducing caseload burdens on administrative authorities and courts and providing an expedited resolution to minor offenses, it can be argued that such arrangements resemble a legalized means of purchasing immunity from prosecution. As a result, legal indulgences raise questions about the fairness and legitimacy of automated administrative punishment, particularly in cases where financial considerations strongly influence one's decision to settle an alleged offense outside of formal prosecution.

Another legal tool facilitating automation of decision-making is the objectification of vehicle owner's administrative liability, coincidentally also stipulated by the Czech Road Traffic Act[22]. By introducing the obligation of the vehicle owner to «*ensure that the driver's obligations and the traffic rules are complied with when using the vehicle on the road*» going hand-in-hand with the administrative offence of failing to do so, the Czech legislator effectively emptied the subjective aspect of the administrative offence (*mens rea*), hence defying the

basic principles of criminal law. Even though administrative punishment is generally considered criminal proceedings under Art. 6 of the European Convention on Human Rights[23], objectivization of administrative liability of vehicle owners surprisingly survived the review by both the Supreme Administrative Court[24] and the Constitutional Court[25], meaning that vehicle owners can be liable for administrative offences they did not commit.

4. Incentives behind automated decision-making

While the expansion of automated administrative punishment *prima facie* appears to be a natural response to modern governance challenges, with automated systems being framed as a neutral technological advancement aimed at increasing compliance through higher detection rates and expedited processing of violations, at the same time it is hard to ignore further factors underlying the issue. When rationalizing the introduction of legislative instruments enabling and facilitating the automation of administrative punishments, policymakers emphasize its potential to enhance enforcement efficiency, ensure consistent application of the law, and alleviate the administrative burden of public authorities, a closer examination reveals a more intricate web of incentives driving the adoption of these systems – ones that extend far beyond mere efficiency.

It is rather obvious that economic considerations play a significant (if not dominant) role in the proliferation of automated enforcement mechanisms. The revenue-generating potential of these systems can hardly be overlooked[26]. Many jurisdictions have faced criticism for using automated traffic fines as a revenue-generating mechanism rather than a purely safety-driven initiative[27]. The self-financing nature of these systems certainly raises concerns about the potential for over-enforcement and a shift in priorities from public welfare to fiscal efficiency, that is issues that extend beyond traffic regulation and into other areas of automated administrative punishment. The prioritization of financial returns may lead to excessive reliance on automated punishment as a revenue stream, potentially incentivizing over-enforcement or reducing the willingness of authorities to apply discretionary leniency.

It is, of course, not inherently problematic for public administration to adopt economically rational approaches. Like any organization, governmental bodies

must ensure they operate within their financial constraints and allocate resources effectively[28]. Efficiency in enforcement, reduction of administrative burdens, and cost-conscious decision-making are all legitimate and even necessary objectives for a well-functioning public sector. However, it should be borne in mind that public administration is not a for-profit enterprise, and its primary function is to serve the public interest rather than maximize revenue. While economic principles can inform and improve decision-making, they should not become the sole driving force behind enforcement mechanisms. When efficiency and financial considerations begin to overshadow fairness, proportionality, and fundamental constitutional principles (especially when it comes to quasi-criminal area of administrative punishment), the legitimacy of the administrative process can be called into question. Striking the right balance between economic rationality and the fundamental principles of justice is crucial to ensuring that automation in administrative punishment serves its intended purpose without undermining its legitimacy.

Ultimately, the debate over economic incentives in automated enforcement is not about whether they are inherently good or bad, but rather about how they are structured and applied in individual cases. A well-calibrated system can leverage financial considerations to improve enforcement efficiency while maintaining the legitimacy and ethical foundation of administrative law. Striking the right balance ensures that automation remains a tool for public benefit rather than a mechanism that prioritizes financial gain at the expense of fundamental rights. Achieving this balance requires a nuanced approach to designing and implementing automated enforcement mechanisms. If economic efficiency is pursued without sufficient safeguards, this comes with a risk of public authorities prioritizing revenue generation and expediency over fairness and justice. The key, therefore, is to integrate economic rationality in a way that enhances administrative functionality without compromising the core values that underpin legal systems.

Another major factor influencing the adoption of automated administrative punishment is the struggle of administrative authorities to carry their burden of proof in traditional proceedings. Due to resource constraints, procedural complexities, and the necessity of human oversight, many authorities find it difficult to meet the evidentiary requirements needed for formal prosecution.

Automation provides a convenient workaround, allowing authorities to bypass intricate investigative processes and shift enforcement models toward preemptive compliance rather than adjudication. By reducing the need for human intervention and streamlining evidentiary processes, automated systems enable authorities to impose sanctions with minimal administrative effort, effectively shifting the balance of power away from the accused and toward the enforcing agency. The problematic nature of this motivation is self-explanatory: while the struggle to increase the efficiency of administrative punishment practices per se is legitimate and even support-worthy, such measures should not be implemented in a manner violating the constitutionally guaranteed rights of administrative procedure parties.

5. Risks of economically incentivized administrative practices

Having established that the automation of administrative punishment practices is at least partially incentivized by fiscal and practical reasoning, it is necessary to critically examine the risks associated with such motivations to ensure that administrative punishment serves its intended purpose without compromising fundamental rights. While some risks are specific to certain types of measures (such as public–private partnership projects[29]), other ones are fairly universal.
In their paper from 2005, Amanda Delaney, Heather Ward and Max Cameron argue that automated law enforcement can be burdened by several problems referred to as "dilemmas". Specifically, automated decision-making can be associated with the «*credibility dilemma*» (see above), the «*social dilemma*», the «*legitimacy dilemma*» and the «*implementation dilemma*»[30]. Those areas can be used as a starting point for the analysis of risks brought by the automation of administrative punishment. The credibility dilemma in automated law enforcement arises from the perception that speed camera programs prioritize revenue generation over road safety, especially in their early stages before safety benefits become evident. The authors of the study argue that over time, enforcement programs in places like Victoria and Britain have shown that public perception may shift to recognizing a dual role, *i.e.* both revenue raising and safety enforcement. The social dilemma stems from the common belief that

minor speeding does not significantly increase crash risk and hence should not be prosecuted. The legitimacy dilemma arises from concerns about fairness and due process compared to traditional enforcement. The implementation dilemma arises from concerns that it diverts police resources from addressing more serious criminal offenses. A related issue is that automation reduces manual enforcement, which is essential for detecting other forms of reckless driving that may be more dangerous than speeding.

Following the use-cases of the legal instruments described afore and assessing their impact on human behavior and administrative practices, several risks can be identified and anticipated. The most obvious risks concern the model of profit-driven enforcement which can, in extreme cases, lead to the abuse of power. Obsession with revenue increase have led to several scandals in the past, with the most notorious ones being the cases of public officials being rewarded based on the amount of imposed fines. This was the case with Rio de Janeiro, in 2021, when the City Hall implemented a policy granting bonuses to employees if the city increased its revenues from electronic traffic fines by up to 65.28% over the 2021 budget[31]. Another infamous example of such practice can be found in Atlanta, Georgia, USA, where the 2022 investigation revealed an incentive system that encouraged police officers to write more tickets[32].

Another branch of profit-driven corruption risks also lies in outsourcing or privatization of administrative penalization. In 2019, the town of Varnsdorf in the Czech Republic became embroiled in a significant corruption scandal involving automated speed enforcement. Mayor Stanislav Horáček and Deputy Mayor Josef Hambálek were implicated in a scheme where they awarded a contract to the company Water Solar Technology for operating speed cameras. The agreement stipulated that the company would receive approx. 12 euros for each issued fine. Within a year, the company issued nearly 60.000 fines, totaling approximately 720.000 euros, far exceeding the contract's stipulated limit and the rationally expected amount. This arrangement violated public procurement laws, leading to legal action against the town's officials[33]. The scandal highlighted concerns about the improper financial incentives associated with automated speed enforcement and the potential for corruption when private companies are remunerated based on the number of fines issued.

While the above-mentioned cases are rather extreme, even common practices are

associated with various risks. When looking at the phenomenon of legal indulgences and their use in practice, it can be argued that this tool not only violates the traditionally subjective nature of administrative offences, but also causes quite a lot of collateral damage along the way. Firstly, it is at least questionable whether such practice can at all fulfill the core objectives of administrative punishment.

The fundamental purpose of administrative sanctions is to deter unlawful conduct, ensure compliance with legal standards, and, where necessary, penalize individual offenders. However, legal indulgences deviate from these principles by shifting the burden of punishment from the actual offender to the owner of the vehicle, effectively disconnecting enforcement from the principle of individual accountability. Instead of ensuring that the person responsible for the infraction is held accountable, legal indulgences operate primarily as a financial transaction between the administrative authority and the vehicle owner. This approach to an extent reduces punishment to a revenue-generating mechanism, where the primary concern is securing payment rather than enforcing behavioral change in the actual offender. Since the legal obligation to pay the imposed amount is placed on the vehicle owner (who may not have committed the violation) the deterrent effect on the real offender becomes secondary at best.

This misalignment with the principles of administrative punishment raises several concerns. First, by imposing financial liability on the owner instead of the driver, the system undermines the fairness of the enforcement mechanism. A core tenet of legal punishment is the idea that sanctions should be proportionate to the wrongdoing and directly attributable to the responsible individual. However, legal indulgences create a scenario where a person who has not committed any wrongdoing is penalized, while the actual offender faces no direct consequences. Second, this practice significantly diminishes the preventive function of administrative sanctions. The purpose of punishment is not merely to impose penalties but to shape behavior and discourage future violations. If a driver knows that a traffic offense will not personally affect them, but rather the vehicle owner, they may have little incentive to adjust their conduct. In this way, legal indulgences fail to serve as an effective deterrent. Furthermore, the decision-making processes of parties to administrative proceedings are also influenced and, in a way, corrupted by the automation, as vehicle owners may opt to pay the

specified amount simply to avoid the legal costs and administrative burdens associated with contesting the penalty, even if they believe they are in the right. The prospect of navigating an often complex and time-consuming appeals process can be daunting, leading many to conclude that settling the *de facto* fine is the more pragmatic choice[34]. This can create an environment where legal challenges are discouraged, undermining the principles of due process and reinforcing a system where financial expediency takes precedence over legal fairness.

The obsession with efficiency can also lead to administrative authorities choosing to follow the most cost-benefit rational path, while leaving some potentially harmful offences uninvestigated. Complex, resource-intensive investigations into serious but harder-to-prove offenses may be deprioritized in favor of automated mechanisms that generate immediate revenue with minimal administrative effort. This may create a perverse incentive structure in which authorities focus disproportionately on minor infractions that are easy to detect and penalize, while more significant but labor-intensive violations go uninvestigated. Consequently, public administration risks shifting from a system of comprehensive regulatory enforcement to one where enforcement priorities are dictated by financial expediency rather than the broader interests of justice and public safety. The take-it-or-leave-it nature of automated decisions and inability of systems used for administrative punishment to effectively exercise discretion also means that imposed sanctions are neither personalized nor tailored based on the specific circumstances of the case.

The harmful nature of this phenomenon can also be increased by the snowball effect leading to more offenders choosing to “fly under the radar” and take advantage of the fact that their behavior goes unpunished. As this pattern continues, it can lead to an erosion of compliance within society. When individuals perceive that certain offenses are effectively ignored by enforcement authorities, they may begin to disregard legal obligations more broadly, assuming that their infractions will also go undetected. This can have serious long-term consequences, as the perception of a weak or selective enforcement system undermines both deterrence and the rule of law. Over time, this lack of consistent enforcement may lead to a decline in general public trust in administrative institutions, as citizens come to view the legal system as one that

prioritizes financial gain over genuine regulatory effectiveness.

6. *Quo vadis*, smart punishment?

The outlooks regarding automated administrative punishment are relatively uncertain, with the future trajectory of depending on complex sociological phenomena and on how policymakers and legal institutions will manage to navigate the tension between efficiency and justice. When it comes to the effectiveness of smart administrative punishment, it is safe to conclude that their effect is generally positive, at least for now. For the purposes of prediction of further development, it is probably better to extract information from the individual parts of the system rather than looking at it from the mountain view. For instance, in terms of deterrence effect, the opinions on whether automated systems are superior to manned traffic enforcement are mixed. The study conducted by Richard Tay suggests that manned enforcement provides greater specific deterrence of high-risk drivers, thus potentially reducing total and serious crashes, while automated enforcement provides a general deterrence effect on a broad spectrum of the driving population, where some effect on the total number of crushes can be observed[35]. Other studies show that fully automated systems can bring underwhelming results by failing to impact people's driving behavior and increase the road safety[36]. Conflicting signals like that somewhat change the perception of the generally upward trend and may indicate possible problems in the future.

Interestingly enough, one of such trends can be observed in the phenomenon where some behaviors related to automated decision-making become economically irrational. For example, a significant number of people seem to deny the authority of automatically issued decisions as opposed to decisions issued by a human being. This finding is also supported by the perception of fines issued by the City of Prague, where lower fines issued by robots were less likely to be paid than much higher fines imposed by humans, which can be explained by the general assumption that while automatically-issued fined can be ignored with a low probability of any negative consequences arising in the future, human officials are more likely to prosecute the non-compliance[37]. This anticipates a sociological phenomenon when the efficiency of automated

decision-making may actually decline over time, once more people realize that they can simply ignore decisions issued by robots since those decisions are not likely to be upheld and enforced by people due to its inefficiency.
While the rise of automated administrative punishment is an undeniable trend, there remains a significant lack of comprehensive data to predict its long-term societal impact and public acceptance accurately. The use of automated enforcement mechanisms is still in a relatively early stage, and while some studies have highlighted concerns over fairness, transparency, and public trust, there has not yet been sufficient longitudinal research to determine how these systems shape public perceptions and behaviors over time. Questions remain as to whether societies will ultimately accept automated enforcement as a fair and impartial means of regulation or whether backlash against perceived overreach will lead to significant pushbacks and demands for reform. The absence of robust data does not, however, change the reality that smart punishment systems are here to stay. The increasing digitization of governance, the growing availability of enforcement technologies, and the financial incentives driving their adoption ensure that automation will likely continue to play an expanding role in administrative punishment, hopefully accompanied by the public debate shifting toward refining the systems, introducing stronger oversight mechanisms, and ensuring that automated decision-making aligns more closely with principles of justice and due process.

7. Possible solutions and considerations *de lege ferenda*

While it is neither the ambition nor the place of this article to formulate comprehensive proposals addressing the aforementioned problems, it is possible to outline the key ideas leading towards the legislative and implementational solutions.
The first critical policy response that naturally comes to mind lies in the principle of revenue neutrality. This concept can and should be adapted to the domain of administrative enforcement as a mechanism to prevent perverse incentives and to reinforce the legitimacy of automated sanctioning systems. Revenue neutrality, in this context, implies that the primary goal of automated enforcement should be behavioral compliance and public welfare, rather than revenue generation.

Under a revenue-neutral framework, any financial proceeds obtained from fines or penalties would be decoupled from the operating budgets of the enforcing authorities. Instead of flowing directly into the coffers of local municipalities, police departments, or private contractors, fine revenues could be redirected into earmarked, independent funds dedicated to road safety education, legal aid, system maintenance, or other public-interest initiatives.

Such a model has two distinct advantages. First and foremost, it undermines the perception (and often the reality) of profit-driven enforcement, thereby restoring public trust. When citizens are aware that automated fines are not being used to finance municipal deficits or to reward officials, the legitimacy of the sanctioning system is significantly enhanced. Second, it dampens the incentive for authorities to over-enforce or manipulate sanctioning thresholds in order to maximize fiscal return. This structural firewall ensures that policy decisions surrounding the deployment of smart punishment systems are made on the basis of safety, fairness, and proportionality rather than short-term budgetary considerations.

To operationalize revenue neutrality, legislatures could impose mandatory budgetary separation rules, which would prohibit fine revenues from being used to fund the same entity responsible for issuing the fines. Additionally, transparency obligations could require periodic publication of enforcement data, revenue flows, and their subsequent uses, enabling public scrutiny and reinforcing democratic control. It is important to emphasize that the adoption of revenue neutrality does not mean that enforcement systems must operate at a loss or forego efficiency. Rather, it insists that financial viability must not come at the expense of justice. Hence, the objective is not to eliminate revenue altogether but to recontextualize it as a by-product of lawful behavior modification, rather than as a primary metric of policy success.

Another systemic solution that can be put in place is the re-personalization of the administrative punishment. One of the most troubling implications of smart administrative punishment, particularly in its traffic enforcement applications, is the increasing detachment between the sanctioned subject and the actual offender. The widespread practice of objectifying liability may simplify enforcement, but it does so at the cost of undermining the core principles of justice, including the presumption of innocence and the requirement of subjective culpability (*mens rea*). To rectify this structural distortion, a shift

toward personal liability tools is needed. These tools seek to reconnect sanctions with the actual conduct of identifiable individuals, thereby restoring the moral and legal foundations of administrative punishment. A straightforward approach is to enhance mechanisms that allow for the identification of the actual offender, which of course might not be always technically possible without a human in the loop.

Further defining features of smart governance should be its capacity to learn, adapt, and self-correct. However, many current models of automated administrative punishment remain static by design, predicated on assumptions of stable compliance behavior, unaffected by long-term sociological and psychological responses. As such, they risk becoming obsolete or even counterproductive over time if they fail to respond to emerging behavioral patterns or declining enforcement efficiency. A striking example of this is the phenomenon where individuals begin to ignore automatically issued fines or administrative notices, under the assumption that automated decisions are either not followed up or are more likely to be unenforced than those issued by human officials. This behavioral loophole, if left unaddressed, can undermine the entire deterrent effect of automated enforcement, transforming it from an efficient tool into an ineffective symbolic gesture. To counter this, administrative authorities must adopt a model of continuous monitoring, empirical assessment, and adaptive intervention. This approach recognizes that enforcement systems operate within dynamic social contexts and must evolve accordingly to remain effective and legitimate.

As a matter of implementation of this approach, authorities could collect and analyze longitudinal data on payment rates, appeals, and behavioral changes associated with automated decisions. Patterns of noncompliance, especially when concentrated around specific types of violations, geographic areas, or technologies, can indicate weak points in the enforcement chain. A noticeable decline in voluntary compliance may signal the erosion of perceived legitimacy or the failure of enforcement follow-through.

Where systemic avoidance of automated decisions is detected, authorities can implement targeted reinforcement strategies to restore the credibility of the system, which could include randomized human follow-up checks, strategic prosecution of ignored fines to signal seriousness, or temporary escalation to

manned enforcement in high-noncompliance zones. Automated enforcement systems should be designed with flexible thresholds, sanctioning schemes, and intervention triggers, allowing parameters to be adjusted based on periodic evaluations. For example, detection algorithms may be fine-tuned based on seasonal or behavioral changes, and penalty amounts could be scaled according to observed deterrence outcomes.

Although we appear to be a long way from the desirable system of automated administrative punishment, with thoughtful design, transparent oversight, and a commitment to aligning technology with fundamental legal principles, it is possible to transform automated enforcement into a just, proportionate, and trusted component of modern smart city governance.

8. Conclusions

The increasing reliance on automation in administrative punishment highlights an inherent tension between efficiency and fairness: the two principles that seem to not always align. On the one hand, economic considerations should not be entirely dismissed when shaping administrative practices, since efficiency is a fundamental objective of administrative governance, ensuring that enforcement mechanisms operate smoothly, cost-effectively, and without undue delays. However, the pursuit of efficiency often comes at the cost of fair process, proportionality and discretion. This tension becomes particularly problematic when financial incentives enter the equation. The drive for efficiency, when coupled with revenue-generation motives, threatens to transform administrative punishment from a tool of regulatory compliance into a mechanism for financial exploitation. When authorities prioritize quick and cost-effective fine collection over nuanced legal adjudication, the enforcement process can become detached from its original purpose of ensuring lawful conduct through just and proportionate penalties.

The concept of "legal indulgences" enshrined by the Czech traffic enforcement legislation serves as the prime example of prioritization of efficiency over basic principles of administrative punishment. At its core, administrative punishment is intended to deter unlawful conduct and impose proportionate sanctions on offenders, while upholding legal certainty and fairness. Legal indulgences,

however, subvert these objectives by shifting the focus from punishing the actual offender to merely resolving the issue in the most administratively expedient manner. Rather than ensuring that those who break the law face appropriate consequences, this model transforms administrative enforcement into a transactional process that prioritizes rapid resolution over genuine accountability, allowing administrative authorities to bypass the burdensome yet essential elements of administrative proceedings.

Prioritization of efficiency has broader implications for the legitimacy of administrative enforcement. When individuals perceive that the system is designed primarily to extract financial penalties rather than to uphold justice, trust in public administration erodes. Legal indulgences, by their very nature, send the message that the goal of enforcement is not to ensure compliance with the law but rather to streamline revenue collection. Over time, this can contribute to public cynicism toward regulatory authorities and diminish respect for legal norms, ultimately undermining the very objectives that administrative punishment is meant to obey. Just as it is fairly easy for a ski descent to turn into an uncontrollable downhill slide from an icy or slippery slope, it is just as easy for the automated administrative practice to go south, should the metaphorical skier-in-the-loop lose their metaphorical grip and fail to carve the curve in a timely manner.

Based on the performed research, the author concludes that some automated decision-making tools in the field of administrative punishment fail to fulfill their primary intended purpose, instead deviating towards secondary objectives such as efficiency or economic rationale. This imposes significant risks on the system as whole, since deviation from basic principles of administrative punishment tends to shift and corrupt the behavior of both administrative authorities and the addressees of legal norms, leading to the state of rational apathy.

Automation will likely remain a defining feature of administrative enforcement in the foreseeable future. Whether it is used to promote justice and compliance or becomes a source of legal controversy will depend largely on the regulatory frameworks and institutional safeguards put in place to manage its risks.

1. The research presented in this article was carried out as part of the 4EU+ project No. MA/4EU+/2024/F3/04 titled «*Charting the Course Towards a New Legal*

Framework for Smart Cities» carried out at the Faculty of Law off Charles University. The author would like to thank Jakub Handrlica and Alessia Monica for their kind support and patience throughout the publication process.

2. See e.g. A. Delaney, H. Ward, M. Cameron, *The History and Development of Speed Camera Use*, Report No. 242, Monash University, Victoria, 2005, or European Commission, *Speed Enforcement Report of the Directorate-General for Mobility and Transport*, in *https://road-safety.transport.ec.europa.eu/eu-road-safety-policy/priorities/safe-road-use/safe-speed/archive/speeding/speed-limits/speed-enforcement_en*, accessed on 18.12.2024.
3. This term is not generally used and is exploited by the author as a wordplay and in alignment with the topic of Smart Cities for the purposes of this article.
4. See e.g. K. Schubel, *U.S. Treasury's AI is Catching Tax Cheats and Saving Billions*, Kiplinger, New York, 2024. See also O. A. Adelekan, et al., *Evolving Tax Compliance in the Digital Era: a Comparative Analysis of AI-Driven Models and Blockchain Technology in U.S. Tax Administration*, in *Computer Science & IT Research Journal, 5 (2)*, 2024, pp. 311-335.
5. See e.g. F. Merli, *Automated Decision-Making Systems in Austrian Administrative Law*, in *CERIDAP, 1, 2023*, Milan, 2023.
6. A. Delaney, H. Ward, M. Cameron, *The History and Development of Speed Camera Use*, Report No. 242, Monash University, Victoria, 2005.
7. See e.g. S. Rahman, R. S. Khan, M. Sirazy, R. Das, *An Exploration of Artificial Intelligence Techniques for Optimizing Tax Compliance, Fraud Detection, and Revenue Collection in Modern Tax Administrations*, in *International Journal of Business Intelligence Research*, vol. 7, no. 3, 2024, pp. 56-80.
8. See e.g. Z. Zuo, *Automated Law Enforcement: An assessment of China's Social Credit System (SCS) using interview evidence from Shanghai*, in *Journal of Cross-disciplinary Research in Computational Law*, vol. 2, no. 1, 2024.
9. See C. Corbett, *Road traffic offending and the introduction of speed cameras in England: The first self-report survey*, in *Accident Analysis & Prevention*, vol. 27, no. 3, 1995, pp. 345-354.
10. See e.g. P. Pilkington, S. Kinra, *Effectiveness of speed cameras in preventing road traffic collisions and related casualties: systematic review*, in *BMJ*, vol. 330, 2005, pp. 331-334, or E. De Pauw et al., *An evaluation of the traffic safety effect of fixed speed cameras*, in *Safety Science*, vol. 62, 2014, pp. 168-174.
11. See e.g. C. Wilson, C. Willis, J. K. Hendrikz, R. Le Brocque, N. Bellamy, *Speed cameras for the prevention of road traffic injuries and deaths*, in *Cochrane Database of Systematic Reviews*, no. 10, 2010.
12. Interested readers can be referred e.g. to S. Kaduk et al., *The use of automated information systems in the investigation of criminal offences*, in *Amazonia Investiga*, vol. 12, no. 61, 2023, pp. 307–316.
13. See J. Nešpor, *Automated Administrative Decision-Making: What is the Black Box*

Hiding?, in *Acta Universitatis Carolinae Iuridica*, vol. 70, no. 2, 2024, pp. 69-83.

14. As a matter of example, the entire Czech system of administrative punishments revolves around the so-called material aspect of the offence, meaning that the administrative authority is obligated to exercise discretion and assess whether the given act fulfils the characteristic of social harmfulness. See Sec. 5 of the l. no. 250/2016 coll., on Liability for Administrative Offences and Proceedings Thereon.
15. A real-life example of this model can be found e.g. in Saudi Arabia, where the so-called Saher System is implemented and used. See Ministry of Interior, Kingdom of Saudi Arabia, *The Saher System*, *https://www.moi.gov.sa/wps/portal/Home/sectors/publicsecurity/traffic/contents/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDTxNTDwMTYy83V0CTQ0cA71d_T1djI0MXA30g1Pz9L30o_ArApqSmVVYGOWoH5Wcn1eSWlGiH1FSlJiWlpmsagBlKCQWqRrkJmbmqRoUJ2akFukXZLuHAwCkY5qs/*, accessed on 23.12.2024.
16. In theory, this is the case of the Czech traffic legislation, at least when it comes to ordinary administrative proceedings (see further).
17. This ironic label refers to the infamous practice of the Catholic Church during the Medieval period when the indulgences (*i.e.* grants reducing or entirely pardoning the punishment for sins) were simply sold and purchased for money, hence enabling the sinners to "bail out" of punishment.
18. L. n. 361/2000 coll., on Road Traffic and Amendments to Certain Acts (Road Traffic Act).
19. Although the Road Traffic Act strictly speaking distinguishes the terms "owner" and "operator", with the latter referring to the person legally operating (not driving) the vehicle on a long-term basis, the term "operator" seems rather confusing in the English translations and may be easily confused with the term "driver" (also used by the Road Traffic Act and referring to the person physically driving the car). For this reason, the author prefers to use the term "owner", which in this case has no impact on the meaning of the communicated message.
20. Sec. 125h para. 1 and 5 of the Road Traffic Act (adapted translation of the author).
21. Since legal indulgences are extraprocedural by design and the sum offered by the administrative authority is not considered a penalty, the *reformatio in peius* principle does not apply and hence fines imposed in the following administrative proceedings can be much higher. In practice, the gap between the requested payments and fines was becoming increasingly smaller and as of today, the difference between the two in most cases is not significant. However, administrative authorities issuing decisions in formal proceedings also impose an obligation to pay the costs of the proceedings, which in many cases can be greater than the fine itself. Thus, taking the indulgence still remains somewhat economically rational.
22. See Sec. 10 para. 3 in conjunction with Sec. 125f para. 1 of the Road Traffic Act.
23. See e.g. European Court of Human Rights, *Lauko v. Slovakia*, judgement of 2 September 1998, 26138/95, or European Court of Human Rights, *Engel et al. v. the Netherlands*,

judgement of 8 June 1976, 5100/71; 5101/71; 5102/71; 5354/72; 5370/72. In the context of the Czech Road Traffic Act see e.g. Supreme Administrative Court of the Czech Republic, Judgment of 16 October 2024, 6 As 237/2023-31.

24. Supreme Administrative Court of the Czech Republic, judgement of 22 October 2015, 8 As 110/2015-46.
25. Constitutional Court of the Czech Republic, ruling of 16 May 2018, Pl. ÚS 15/16.
26. C. Sun, *Is Robocop a Cash Cow? Motivations For Automated Traffic Enforcement*, in *Journal of Transportation Law, Logistics, and Policy*, vol. 78, no. 1, 2011, pp. 11-35.
27. This issue is often referred to as the credibility dilemma, see e.g. A. Delaney, H. Ward, M. Cameron, *The History and Development of Speed Camera Use*, Report No. 242, Monash University, Victoria, 2005, p. 7.
28. An example of a good economically-conscious practice can be found in de minimis thresholds in certain offences or value limits used in customs administration ensuring that scarce resources are not used on minor activities with no significant impact on the system.
29. See e.g. M. Gerrard, *Public-private partnerships*, in *Finance and development*, vol. 38, no. 3, 2001, pp. 48-51.
30. See A. Delaney, H. Ward, M. Cameron, *The History and Development of Speed Camera Use*, Report No. 242, Monash University, Victoria, 2005, p. 9.
31. The Rio Times, *Rio de Janeiro city government to reward traffic officials for issuing more fines*, in *https://www.riotimesonline.com/brazil-news/rio-de-janeiro/rios-city-hall-to-reward-public-servants-for-issuing-more-fines/*, accessed on 7.1.2025.
32. The system was structured as a point-based mechanism, where officers accumulated points for various activities, including issuing citations, which could influence evaluations and promotions. See R. Polansky, *Are Atlanta officers incentivized to write more tickets? CBS46 Investigates*, in *Atlanta News First*, 2024.
33. See e.g. Děčínský deník, *Kauza radarů ve Varnsdorfu*, in *https://decinsky.denik.cz/tema/kauza-radaru-ve-varnsdorfu.html*, accessed on 7.1.2025.
34. It must be also noted that, in many jurisdictions, the parties are not entitled to any reimbursement of legal costs in administrative proceedings, even if the charges are dropped and the accused offender is found not guilty.
35. R. Tay, *The Effectiveness of Automated and Manned Traffic Enforcement*, in *International Journal of Sustainable Transportation*, vol. 3, no. 3, 2009, pp. 178-186.
36. See e.g. H. Al-Shammari, C. Ling, *Investigating the Effectiveness of a Traffic Enforcement Camera-System on the Road Safety in Saudi Arabia*, in *Advances in Human Aspects of Transportation*, 2019, pp. 660-670.
37. See H. Jois, *Evaluating human response to robot-administered punishment*, Pennsylvania State University, University Park, 2021.