Hacker, Philipp; Neyer, Jürgen

Article

Substantively smart cities: Participation, fundamental rights and temporality

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Hacker, Philipp; Neyer, Jürgen (2023) : Substantively smart cities: Participation, fundamental rights and temporality, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 12, Iss. 1, pp. 1-30, https://doi.org/10.14763/2023.1.1696

This Version is available at:
https://hdl.handle.net/10419/271323

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 12 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Substantively smart cities – Participation, fundamental rights and temporality

Philipp Hacker *European University Viadrina Frankfurt* Hacker@europa-uni.de
Jürgen Neyer *European University Viadrina Frankfurt* neyer@europa-uni.de

DOI: https://doi.org/10.14763/2023.1.1696

Published: 31 March 2023
Received: 16 September 2022 **Accepted:** 2 December 2022

Funding: Philipp Hacker did not receive any funding for this research; Jürgen Neyer received a grant from Volkswagen Foundation to conduct empirical research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Hacker, P. & Neyer, J. (2023). Substantively smart cities – Participation, fundamental rights and temporality. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1696

Keywords: Smart cities, Data protection, Non-discrimination, Participation, AI governance

Abstract: Smart city applications are increasingly deployed in urban spaces around the world. We contend that they only merit the attribute "smart" if they embody what we term "substantial smartness". To develop this concept, we draw on both political and legal theories to show that citizen participation and activation, as well as respect for human and fundamental rights, are two essential dimensions of substantial smartness. Both dimensions, however, need to accommodate temporality, i.e., rapid changes in deployed technologies, their purposes and citizens' use of public infrastructure. By highlighting three examples and discussing smart city challenges to the GDPR, non-discrimination law and the proposed EU AI Act, we demonstrate that politics needs the law – and vice versa – to unlock the potential of substantively smart cities.

This paper is part of **Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies**, a special issue of *Internet Policy Review* guest-edited by Alina Wernick and Anna Artyushina.

Introduction: Interdisciplinary dynamics of smart environments

Law and politics relate to, and seek to govern, a world of change. Therefore, they are confronted with the challenge of adapting their content and effects over time, and mitigating risks not contemplated at the moment when decisions were made. This disconnect infuses an unavoidable element of temporality into the politico-legal realm. Such dynamics are particularly present in digital information technology, where advances in computer science and novel connections between different technical tools create a protean landscape of ever-changing and increasingly integrated data sets, models and applications. Yet, similarly, political action occurs in this space and may harness digital technology to adapt to, and contest, new practices and risks to human rights.

Such dynamic, politico-legal spaces are epitomised by the so-called "smart city", marked by a constant change in technology and its purpose, and simultaneously by frequent alterations to the use of public infrastructure. The street conceived as a way of transport may suddenly become an avenue of protest. Public space in the city, instrumentally used for commerce, recreation, or movement, may thus be rapidly converted into a space of contestation (Colomb & Novy, 2016). Political protest, after all, typically converges toward cities, where political elites are located, who are often the ultimate audience of protest movements. Conversely, data collected in public spaces is prone to function creep, i.e., fast shifts in the exploitation and purpose of processing (cf. Graham & Wood, 2003; Koops, 2021). The growing deployment of data-collecting sensors in cities, coupled with analytics frameworks, thus has potentially far-reaching consequences. Public infrastructure is unavoidable for city dwellers who need to participate in many essential activities, from shopping to transport (Eckhoff & Wagner, 2017; Kroll, 2022, p. 2). That necessity highlights the need to bring human rights-based legal frameworks (HLEGAI, 2019; Donahoe & Metzger, 2019; Zuiderveen Borgesius, 2020; Yeung et al., 2020) to bear on emergent smart city applications (cf. Edwards, 2016). Indeed, abuse of smart city infrastructure and possible human rights violations are not to be merely attributed to distant dystopias, as the tracking of participants in the Black Lives Matter movement via smart city technology has shown (Artyushina &

Wernick, 2021). Chilling effects on the exercise of individual human rights may ensue.

This threat is illustrated further by a case from San Diego, where smart streetlights were initially installed to collect data on environmental and traffic conditions (Marx, 2020). However, during the Black Lives Matter protests of 2020, they were coupled with face recognition technology (FRT) and used to track protesters for law enforcement purposes (Marx, 2020; see also Edwards, 2016), challenging human rights to data protection, assembly and potentially non-discrimination (Kitchin, 2016). Moreover, entry to public buildings may soon be regulated, not by old-fashioned bells and civil servants checking ID cards, but by identity verification via FRT (Information Commissioner's Office, 2021, p. 12). Such a strategy may initially function well if applied in areas with an ethnically homogeneous population that statistically matches the data that the model was trained with. However, as the deployment of tools is expanded toward more ethnically diverse areas, access may increasingly be erroneously denied to individuals not correctly recognised by the model. As empirical studies suggest, FRT model performance may be significantly lower for black women (Buolamwini & Gebru, 2018; Robinson et al., 2020; Cavazos et al., 2021), raising the spectre of discrimination by misidentification. Hence, the computer might "say no" to a black female citizen wanting to collect her passport, as opposed to her white male neighbour.

Research questions and methods

Cases such as the ones mentioned leave us with a triple research question. First, how can political movements adapt to, and effectively contest, such changing infrastructures in the open space? Second, how can we close the gap between the pace of technological change on the one hand and the sluggishness of the law, which is supposed to regulate it, on the other? And, third, how can the answers we find to the first questions contribute to a refined understanding of "smartness" in the smart city context?

We contend that analyses need to be interdisciplinary to answer these questions in order to accommodate the multifaceted object of inquiry. This paper draws on political and legal theories, as both are deeply affected by temporality in the smart city. Technological innovation may establish new surveillance practices, encroach on civil liberties, threaten fundamental rights and imply a silencing of political activism (Finch & Tene, 2013). But politics and law, as we wish to show, may also mutually reinforce one another. This paper, therefore, explores how regulatory techniques, innovative political practices and novel laws seek, manage, or fail to

accommodate technological change brought about by time's passage and contribute to governing the smart city. We aim to show that the streets of the smart city are politically charged and legally sensitive, and that time is of the essence. In doing so, we focus on the mechanisms for internalising temporality, and on three legal domains particularly relevant for human rights protection and artificial intelligence (AI) regulation in the EU: the GDPR, non-discrimination law and the Artificial Intelligence Act (AIA) proposed in April 2021 and significantly updated in December2022 (Council of the European Union, 2022).[1]

Temporal challenges to human rights in smart cities

In doing so, the paper highlights the challenges produced by deploying technology in smart city contexts (Camero & Alba, 2019), particularly by data-collecting sensors and analytics powered by machine learning (Goodman, 2020; Haque et al., 2021). Having been hailed as the urban form of the future (Hall et al., 2000; Meijer & Bolívar, 2016; Wlodarczak, 2017), smart cities have increasingly faced backlash on a local and a global level, and several renowned smart city projects have been abandoned recently. Toronto is a prime example of such failure (Carr & Hesse, 2020). In 2017, Sidewalk Labs (a subsidiary of Alphabet) won a tender for transforming a 2,000-acre site located directly between Lake Ontario and downtown Toronto. The concept proposed by Sidewalk Labs envisioned an entire new urban district that would apply everything that was technologically possible: from autonomous cars to heated sidewalks, and autonomous garbage collection and traffic flow sensors to the comprehensive data collection of virtually all public activities. The project represented an attempt to realise the utopia of a technology-driven smart city in which citizens would be made as comfortable as possible without being bothered by having to decide on the menu of services being offered. Nevertheless, the project was never realised. Strong public resistance formed from the very beginning and criticised the autonomy of the planning process and its low level of public participation. The company was accused of hubris, arrogance and a disregard for democratic standards in the planning process. In the spring of 2020, two weeks before the competent local authority was to decide on its realisation, Sidewalk Labs terminated work on the project and withdrew from all further planning.

The case is instructive for understanding the local conditions of legislative temporality. If technological change is to be realised in urban contexts, the process designers are well advised to engage citizens; the more, the better. It shows that technology alone is insufficient to motivate social action, but it runs into open op-

1. All AIA references in this paper refer to this December 6, 2022 version (Council, general approach).

position if companies attempt to implement it top-down without citizen participation (cf. Artyushina & Wernick, 2021). Nevertheless, while fully integrated smart cities remain a vision rather than a reality (Hankin, 2022, p. 2), specific elements of smart city applications – from adaptive streetlights to video surveillance, from integrated traffic control to autonomous and connected vehicles – continue to be deployed at a rapid pace. This trend is likely to be accelerated even further by the incentives set by the EU Commission's investment package offering special funding for cities in exchange for installing smart green technology (European Commission, 2021, p. 127 et seqq.).

Smart technology deployed in urban environments compels the law and politics to deal with risk and uncertainty concerning the future development, application and functioning of data-driven tools embedded in public infrastructure. As the following sections will show, politics and the law react in different but mutually dependent ways to the phenomenon of temporality in the smart city context. Both start from the premise that the dynamic nature of technology makes it nearly impossible for legislators to adopt laws at the same pace as technology proceeds (Fairfield, 2021; Bennett Moses, 2016). The political reaction, however, is often *external* to the existing law. It may take the form of political discourse and activism, seeking to contest and change the law, or of strategies to fine-tune and adapt its current implementation on the ground. In either case, reactions to dynamic changes in the technological environment will often take the form of *local* action in specific (smart city) communities. Here, technological changes are most acutely and rapidly felt; and local implementations can often be changed more easily than entire regulations.

Substantive smartness

To function effectively, however, the law arguably needs politics and politics need the law, particularly under conditions of temporality. We show this in the smart city context by developing the concept of "substantive smartness". In the political arena, in our view, this entails putting participation in smart environments centre stage (participatory smartness) (cf. Capdevila & Zarlenga, 2015). Citizen involvement is essential for several reasons. First, regulators often lack the resources to monitor developments and effectively enforce laws across a diverse array of implementations (Kaminski, 2023, p. 79). Second, to paraphrase criminal justice reformer Glenn Martin, those closest to harm are often closest to the solution (2017; see also Metcalf et al., 2021, p 743). They gather experience via direct contact with the technologies on the ground and may engage in dialogue with one another to discuss solutions. Digital formats of exchange may significantly facilitate such de-

bates.

Barcelona and Madrid are often cited as strong examples of close citizen participation (Charnock, March & Ribera-Fumaz, 2021; Smith & Martín, 2021). The smart city process started in Barcelona and Madrid in the early 2010s. Both approaches were built on an IT strategy that used open data platforms that aimed to generate participatory processes. A cornerstone of the strategy was the introduction of online platforms for citizen participation. *Consul* in Madrid and *Decidim* in Barcelona offered a space for citizens to engage city-wide or on a more limited scale to organise local meetings, roundtables and offline walks, as well as online interactions, such as requests for comments, proposals and information gathering and posting videos of meetings on the platform. The use of the platforms was not limited to informal citizen deliberations but was closely connected to authoritative decision-making. The Municipal Action Plan in Barcelona (2016-2019), for example, which is the roadmap for the City Council's policies, was the first use of the Decidim platform. It is also worth noting that the two online platforms for citizen participation are not ready-made implants into the political process, but are constantly redesigned to improve functionality. In Barcelona, a Metadecidim lab provides a public forum for debating the platform, its design, use and governance processes. This has recently been expanded into a Laboratori d'Innovació Democràtica funded by the Council. In Madrid, Participa Lab, based at Medialab-Prado (a public centre for digital culture), has played a similar role.

Both platforms are thus subjected to citizen scrutiny and provide opportunities to not only use participatory processes but to design and redesign them as seems fit to enhance urban democracy. The notable success of the two platforms has led to impressive figures. According to Smith and Martín (2022, p. 317), in late 2019, Decide Madrid had 655,559 users registered, with over 27,123 proposals produced and 5,699 debates posted. More than 200.000 comments were published and over four million votes cast. Decidim Barcelona had launched forty participatory processes with 14,481 proposals and 1,105 citizen initiatives. It enabled 32,000 people to participate in formulating the city strategic plan and involved 28,000 citizens making 12,000 proposals on other projects. While not all that glitters is gold, the two projects show that participation in the implementation of technology may be successfully operationalised, even in large communities. Not surprisingly, the two platforms are now widely adopted by other international city authorities.

It is also interesting to note that citizens are often motivated to contribute when their own community is affected. A survey of a total of 663 citizens, conducted in Frankfurt (Oder) by one of the authors in the fall of 2021, showed that a large ma-

jority of respondents supported the overall idea of a smarter city. 71% of all respondents expected digital technologies to make everyday life more manageable, while only a tiny minority of 1.5% saw no advantages to digital technologies. (Neyer & Worschech, 2022). Citizens furthermore expressed a clear interest in being consulted in all critical matters. Nearly every second citizen (46%) expected to be asked to vote on important decisions. As opposed to voting, consultation was supported by only 27% of the respondents, while only 7% were content with being merely informed. These results represent a significant potential for developing participatory smartness.

But dialogue, awareness and participation are hardly enough. In addition, the law must safeguard citizens' human and fundamental rights vis-à-vis smart city applications. Only the law can authoritatively compel AI providers and operators to design and implement smart city applications in line with human and fundamental rights (human rights-respecting smartness) (see also Edwards, 2016; Sadowski & Pasquale, 2015). Ultimately, however, both dimensions of substantial smartness depend on one another: participation without human rights is empty and human rights without participation are blind.

Roadmap

To show this, the paper proceeds in four steps. First, it lays the conceptual foundations of temporality (section 1). Second, we introduce the smart city as a particular space of dynamic contestation, which needs participation and digital networks. In this context, we also touch upon platform regulation, which does not, however, constitute a focus of this paper. Third, we show how the GDPR, non-discrimination law and the AIA proposal grapple with reining in the temporal dynamics of AI development, how they apply in a smart city context and how their provisions contribute to HR-respecting smartness (section 2). Note that certain aspects of the relationship between law and citizen participation, such as public or zoning law, are not addressed due to space constraints. Finally, the paper suggests several tools and principles to recognise, internalise and reconcile the dimensions of temporality in law and politics (section 3). Ultimately, such instruments are crucial to guard against risks the future inevitably confronts us with. The paper concludes with a summary of our findings regarding the idea of "substantive smartness" we have formed, along with the interconnectedness of law and politics.

Section 1: Conceptual foundations of temporality

Temporality is a term with varying content in many fields (see, e.g., the linguistic

overview in Jaszczolt, 2009; see also Ingold, 1993; Khan, 2009; Amin, 2014; Dawson & Sykes, 2019). Generally, in our understanding, it denotes the relationship of a concept, an institution or an individual to the passage of time. In the politico-legal world, temporality takes on a crucial, yet often overlooked dimension as societies and institutions evolve, and political structures as well as legal concepts and systems need to be kept abreast (cf. Bennett Moses, 2016).

More specifically, the meaning and effectiveness of the law itself are often implicitly subject to a temporal dimension (Bennett Moses, 2007; Khan, 2009; Delacroix, 2022). It is a trivial insight that the world, which the law regulates, changes more often and frequently than the wording of the law itself. Regulatory theory has for quite some time stressed the need to adapt to changing circumstances to foster responsive regulation (see, e.g., Black & Baldwin, 2010, pp. 186-187). From a theoretical perspective, we submit, the law may relate to the temporality of its objects in three distinct dimensions, thereby, as it were, "temporalising" itself (see also Fig. 1). First, the law may *explicitly* address the risks of certain specific future developments (*temporality by direct regulation*). This may happen in two distinct ways. On the one hand, a provision might regulate (e.g. proscribe) concrete foreseeable technological implementations which will, however, only be technically realised in the future (*forward-looking regulation*). On the other hand, regulation may compel regulatees to take risks into account when they materialise, even if they cannot be expressly foreseen when legislation is enacted (*adaptive regulation*) (cf. also Armstrong, Gorst & Rae, 2019, p. 20).

Second, if the law does not provide such direct tools, legal institutions may seek to hermeneutically work technological change over time into the content of the law itself. Such *temporality by interpretation* may take the form of *implicit* and *explicit* temporal interpretation. For example, venerable legal concepts may be reinterpreted to assume new meaning in the face of technological change (*implicit temporal interpretation*). This option frequently arises as many legal provisions and concepts are formulated in a technology-neutral way (Bennett Moses, 2007; Yeung & Bygrave, 2022). Thus, the Product Liability Directive (PLD) was introduced in the EU in 1985. A product was defined as "all movables", i.e., only tangible objects, in Art. 2 of the PLD. Today, however, it should arguably be interpreted to include standalone AI, and more broadly, even software (Howells, Twigg-Flesner & Willett, 2017). Similarly, EU non-discrimination directives were largely passed in the year 2000 when lawmakers did not conceive of AI systems delivering discriminatory output. Nevertheless, non-discrimination arguably applies to such AI-facilitated decisions (see, e.g., Hacker, 2018; Wachter, 2020). While such temporalisation oc-

curs implicitly, the law may also explicitly state that future developments need to be taken into account when applying the law (*explicit temporal interpretation*).[2]

The mentioned direct and hermeneutical strategies to cope with temporality leave the letter of the law intact. This is often different in the third type of legal reaction: *temporality by review*. Again, we may distinguish two different subtypes: review may need to be conducted by regulatees, who need to install continuous compliance management systems (*compliance temporality review*), or by legislators, who can effectively change the law (*legislative temporality review*). In the legal arena, temporality, therefore, refers to various strategies to adapt legal norms to changing circumstances concerning the regulated objects – lest the law petrify as a historical artefact and become increasingly obsolete, particularly in scenarios involving IT innovations.

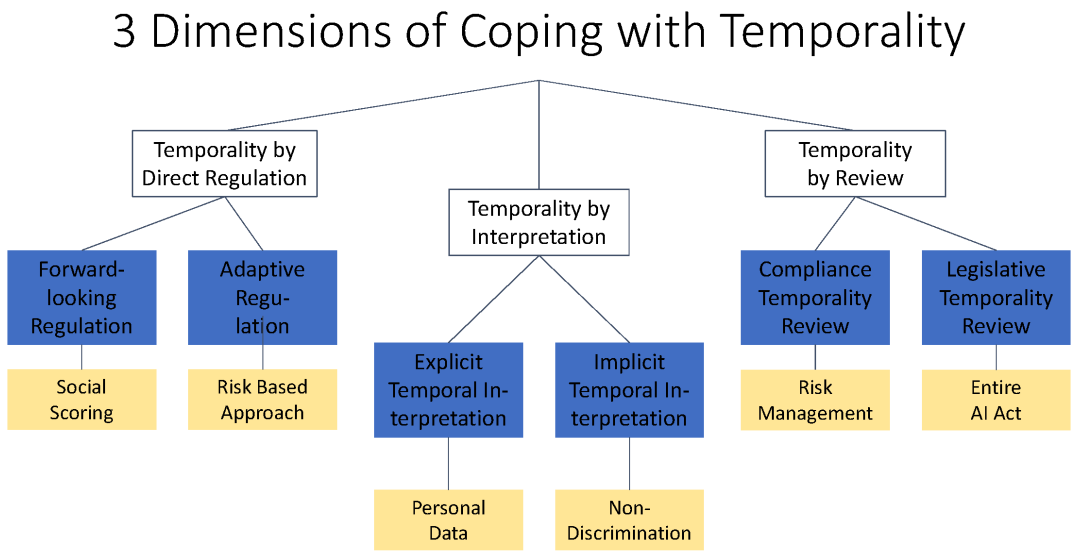

FIGURE 1: An overview of dimensions of temporality in law (Source: Authors' own presentation).

Many scholars in the realm of AI regulation propose that a solid human or fundamental rights-based framework is indispensable for safeguarding the public inter-

2. While adaptive regulation is addressed towards regulatees (e.g., companies), explicit temporal interpretation is primarily conducted by agencies or courts applying (and hence authoritatively interpreting) the law.

est and private liberty in our increasingly algorithmic societies (HLEGAI, 2019; Donahoe & Metzger, 2019; Zuiderveen Borgesius, 2020; Yeung et al., 2020). What is less clear, however, is how such affordances can be operationalised in practice, and how they can accommodate change over time. Importantly, in the EU fundamental rights requirements are spelled out in secondary legislation, such as specific EU directives or regulations: data protection in the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and non-discrimination in various directives. Finally, the EU Commission has proposed the AIA, inter alia, to guarantee fundamental rights protection in the context of deploying machine learning models in public and private settings (cf. Recitals 1, 2, 13 AIA). As we shall see, however, the acts differ vastly in their accommodation of the inherently changing nature of data uses, models and applications.

Section 2: Regulating AI-induced temporality in the smart city – Towards HR-respecting smartness

The political contours of substantive smartness chiefly involved strengthening the participatory system, with robust legal boundaries to mitigate the regressive effects of participation. In its legal version, substantive smartness, in our view, primarily equals respect for human and fundamental rights. In this paper, we cannot review all the fundamental rights at stake (for a broader scope, see, e.g., Kempin Reuter, 2020; Flak & Hofmann, 2020); instead, we will have to restrict ourselves to those most clearly challenged in a smart city context: data protection, non-discrimination and rights/obligations flowing from the proposed AI Act. Through these acts, the law can be understood to foster substantive smartness by limiting surveillance, bias and errors in AI-based smart city contexts. These guarantees are also essential to creating an effective and safe environment for citizen participation (see also section 3). Effectively safeguarding the mentioned rights, however, also implies accommodating temporality again: only by acknowledging the temporal nature of law and the dynamics of technological change can human and fundamental rights be operationalised in a future-proof way.

Participation, legal issues and temporality

The link to temporality also evidences the interwoven character of law and citizen participation in the smart city. In that context, temporality is chiefly induced by technological change or function creep. However, such threats to fundamental rights must first be detected so that adequate responses may be formulated and frictions addressed in the conception or application of the law.

Here, citizen participation plays an important role. The DSA provides various mechanisms to notify platforms of problematic content. Similarly, citizens – and particularly politically active citizens – may inform city authorities and agencies of potentially illegal uses of digital technology in a smart city context. The usefulness of such decentralised mechanisms is well known from the literature on decentralised enforcement (see, e.g., Landes & Posner, 1975; Burbank, 2013). More specifically, tapping the resources of decentralised knowledge may solve information problems arising from limited monitoring capacities in public enforcement bodies (cf. already Hayek, 1945; see also Landes & Posner, 1975; Burbank, 2013).

In this sense, citizen participation is a necessary precondition for effective legal implementation. Furthermore, citizens may also actively contribute to the design of novel solutions, for example in the realm of explanations regarding AI systems or justification structures. Researchers have already pointed to the advantages of using co-design strategies to this end (Liegl et al., 2015), also in AI regulation (Aldewereld & Mioch, 2021; Hacker & Passoth, 2022). Such participatory strategies may then be fused with a legal system willing and able to receive such input and accommodate temporality. The following parts review to what extent the GDPR anti-discrimination law and the proposed AI Act address temporality, in smart city contexts and beyond.

Temporality in the GDPR

In the GDPR, two strategies are pursued to effectively internalise temporality: explicit temporal interpretation and adaptive regulation (cf. also Yeung & Bygrave, 2022). We will analyse the former by examining the GDPR's applicability, which depends on the processing of personal data; and the latter by discussing the GDPR's risk-based approach.

Applicability – explicit temporal interpretation: The GDPR famously only applies if personal data is processed, Art. 2(1) GDPR. This presupposes that individual data subjects can be effectively identified (Art. 4(1) GDPR). Particularly in large data sets, this criterion turns, among other things, on technical strategies of re-identification (Finck & Pallas, 2020, p. 18 et seqq.; Hacker, 2021, pp. 265-268). Since such technical capabilities will change over time (Rocher et al., 2019), the applicability of the GDPR is itself subject to temporality. This was duly noted by the framers of the GDPR, who, in Recital 26, formulated that identifiability must take "into consideration the available technology at the time of the processing and technological developments".

The extent to which such developments must be taken into account remains, however, largely unclear (Shabani & Marelli, 2019, p. 2; Finck & Pallas, 2020, p. 17). For example, some scholars have argued that scanning the faces of otherwise unidentified passers-by and analysing their emotions, does not qualify for identifiability in the sense of the GDPR (Article 29 Data Protection Working Party, 2012a, p. 4; Article 29 Data Protection Working Party, 2012b, p. 16; McStay, 2016, pp. 6-8; McStay, 2020, p. 4). This result is highly problematic as it leaves citizens subject to emotional AI in public places, deprived of the protections of the GDPR (McStay, 2016, p. 6; Veale & Zuiderveen Borgesius, 2021, para. 74; Hacker, 2022, p. 31). However, such analyses may generate large data sets on the involved passers-by. Therefore, one may duly argue that, projecting further advances in technical re-identification strategies, one would have to qualify larger data sets even of otherwise unidentified passers-by as personal data. Failing that, the EU must move quickly to provide specific privacy protection to those affected by body measurements in connected environments (Hacker, 2022, pp. 32-33).

Another example comes from the domain of connected and autonomous vehicles. In a smart city context, they will communicate data concerning their speed, direction, location, traffic conditions and other attributes (Haque et al. 2021, 16 et seq.). Even though the rider's identity is not directly transmitted, it is not unimaginable that the combination of attributes makes drivers identifiable. If, however, the data is encrypted and vehicle identifiers are changed regularly, the chances of re-identification are significantly lowered (Tan & Chung 2019). Nevertheless, future technological advances in areas such as quantum computing (decoding encryption, Atik & Jeutner 2021) or re-identification algorithms (Rocher et al. 2019) may render such additional safeguards obsolete, reintroducing the unique identifiability of actors.

Again, technological progress may therefore render the GDPR applicable even before it has materialised (Article 29 Data Protection Working Party, 2014, p. 9). What must be demanded, under any reasonable interpretation of the concept of personal data, however, is that the developments mentioned in Recital 26 are foreseeable (Schantz, 2016, p. 1843) and will likely occur while the data is still stored (Article 29 Working Party, 2007, p. 15; Finck & Pallas, 2020, p. 16). Breaking asymmetric encryption via quantum computation, for example, is merely theoretically possible at the moment (Garfinkel & Hoofnagle, 2022, p. 1). Hence, it is not sufficiently foreseeable and should not lead to a qualification as personal data. As an additional criterion, the developments must, in our view, be highly likely to occur within a timeframe during which access to the data in question triggers the typical data protection risks for specifically those data subjects whose data is processed (e.g.,

not after data subjects are deceased). These risks are mentioned in Recital 75 GDPR and include, inter alia, "discrimination, identity theft or fraud, financial loss, [and] damage to the reputation".

In our view, such a temporal interpretation strikes a measured balance. On the one hand, it ensures that companies still have an incentive to anonymise data (cf. Hacker, 2021, p. 267): the risk of re-identification must be concrete and not merely hypothetical to bring the data set within the scope of the GDPR. Robust de-identification techniques will, therefore, effectively foreclose the applicability of the GDPR (Recital 26). On the other hand, the precautions demanded by the GDPR must be undertaken now if the purpose of the GDPR – guarding against data protection-specific risks – will very likely be affected by technological developments in the foreseeable future.

Risk-based approach – adaptive regulation: Recital 26 GDPR mentions technological developments, triggering an explicit temporal interpretation. The GDPR, however, does not stop there. Once it applies, temporality must also be taken into account with respect to its substantive provisions. Perhaps the best example is the risk-based approach the GDPR pursues (Gellert, 2015; Lynskey, 2015, p. 81 et seqq.; Clifford & Ausloos, 2018, p. 182-83; Hacker, 2020, p. 14 et seqq. and § 4).

Under such an approach, more significant risks entail heavier regulatory burdens for data controllers (i.e., companies processing the data) (Lynskey, 2015, p. 82). Importantly and in contrast to the temporal interpretation of the concept of personal data, a risk-based approach even covers risks that were not foreseeable at the moment in which the law was enacted (cf. Gellert, 2015, p. 15). It is thus inherently oriented toward the future (Black & Baldwin, 2010, 200). While a risk-based framework is not immune to critique (see, e.g., Black, 2005, 519; Kaminski, 2023, p. 21 et seqq.), it is firmly entrenched in the GDPR and contributes to its adaptive capacity. For example, data protection by design and default (Art. 25 GDPR) and IT security (Art. 32 GDPR) always have to be implemented with respect to the state-of-the-art, in a manner appropriate to the processing risks, at the moment of data analysis. Furthermore, companies must conduct data protection impact assessments when launching novel high-risk processing operations (Art. 35(1) GDPR). Importantly, this assessment needs to be repeated each time the risk represented by the processing changes measurably (Art. 35(11) GDPR).

The GDPR compliance regime, therefore, has a future-oriented character, enabling it to flexibly adapt to changes in the risk structure of processing operations. In the context of smart city instalments, for instance, new mitigation measures have to

be undertaken if it becomes apparent that the data collected by smart streetlights is syphoned off by third parties, prone to hacking, or facilitates systematic surveillance not initially conceived of during implementation. In the San Diego case, the streetlight cameras were installed to capture traffic and environmental data, but they have increasingly been used by law enforcement officials (Marx, 2020). Under EU legislation, this would clearly trigger the need for new data protection impact assessments and related safeguards.[3] Overall, the risk-based approach of the GDPR already puts emerging technological risks centre stage, both in its applicability and its substance.

Risk of future discrimination – Implicit temporal interpretation

Data protection, however, is not the only concern when data is processed in a smart city context. Rather, technology will often serve as a gatekeeper, channelling virtual access to services or even physical access to buildings. To return to our introductory example, imagine that a proactive City Council announces that they will equip the City Hall with face recognition technology (FRT) so that citizens showing up for an in-person meeting can be automatically recognised at the doorstep and granted entry. Such verification systems may become even more plausible, with regulated access, during a pandemic.

As mentioned, however, there is abundant empirical evidence showing that FRT systems tend to underperform vis-à-vis ethnic minorities, and even show significant performance differences between genders (Buolamwini & Gebru, 2018; Robinson et al., 2020; Cavazos et al., 2021). This is often due to the unequal representation of protected groups in training data sets (Cavazos et al., 2021). In our view, the refusal to grant entry to a person from a protected group because of malfunctioning FRT generally constitutes illegal discrimination by the entity responsible for the admission process (Zuiderveen Borgesius, 2020, p. 1577; Hacker, 2018, pp. 1163-1164; Wachter, 2020, pp. 407-412).[4] However, this begs the question of whether EU non-discrimination law is future-oriented to the point that the mere *announcement* of the installation of an FRT system already enables potential victims to stop the process, before the system even becomes a reality.

In a recent case (CJEU, Case C-507/18, *Associazione Avvocatura per i diritti LGBTI*, para. 58), the CJEU affirmed an implicit temporal interpretation of the concept of

3. Note that, in the area of law enforcement, it would have to follow Art. 27 of the Law Enforcement Directive 2016/680; see also the recent EDPB Guidelines (2022).

4. Enforcement problems remain, however (Zuiderveen Borgesius, 2020, p. 1577; Hacker, 2018, p. 1167 et seqq.).

discrimination. It ruled that mere declarations to discriminate at a later point in time may trigger liability under EU non-discrimination law, offering the possibility of injunctive relief to potential victims before the actual discriminatory act takes place. However, as a first prerequisite, it must be clear from the statement that the FRT system will, in fact, have an illegal discriminatory impact upon a protected group. This is clearly the case if the announcement states that a particular system or certain training data sets will be used, which is known to be skewed against certain protected groups. Even in the absence of such details, however, the pervasive empirical evidence of errors and bias in FRT should lead to a presumption – to be rebutted by the prospective operators – that the FRT system will illegally discriminate against protected groups (Kroll, 2022, p. 3). As a second, cumulative prerequisite, the CJEU clarified that the connection between future discrimination and the announcement must be concrete and not merely hypothetical (para. 43 of the judgement; Tryfonidou, 2020, p. 518). As I have explored in greater depth in previous work (Hacker, 2021, pp. 272-274), general statements to use AI or other technology potentially exhibiting discriminatory features are, therefore, not sufficient to trigger liability. Similarly, the mere generic assembly of a data set for machine learning purposes likely does not prompt non-discrimination law scrutiny if it is not clear that it will be used in a setting to which that set of laws applies (cf. para. 40 of the judgement).

As we shall see in the next section, the new Art. 4a-c AIA partially addresses this shortcoming (see next part). To trigger strict liability under non-discrimination law, however, the specific use case must be named or clear from the circumstances (e.g., regulating entry to public buildings). Only the use case establishes the concrete relationship demanded by the CJEU. Non-discrimination law then conveys future-oriented injunctive relief to potential victims of substantively dumb "smart"-city applications.

Temporality in the AIA

Finally, we shall look at how the proposal for an AI Act accommodates temporality and may be used to support a human/fundamental rights-based framework for smart city regulation. The latest version of the proposal now makes repeated references to the risks AI may pose to fundamental rights.[5] As we shall see, the AI Act takes temporality induced by technological change quite seriously. On the most basic level, the proposal distinguishes between banned, high-risk and other AI ap-

5. Note that such references may, however, in the end weaken human rights protection if they establish additional criteria, as in Art. 6(3) AIA concerning the qualification of models as high-risk applications.

plications, with regulatory scrutiny focusing on the former two categories (Veale & Zuiderveen Borgesius, 2021).

Banned AI systems – forward-looking regulation: In its Art. 5, the AIA outlaws certain specific, particularly controversial AI applications, such as social scoring systems, face recognition systems for law enforcement (with certain exceptions), or subliminal influence systems. These are indeed examples of forward-looking regulation as many such systems, like AI-based scoring, have not yet been developed or are not yet used in the EU. This points, however, to a significant shortcoming of Art. 5 AIA: it targets slightly far-fetched, dystopian applications (except FRT) (Veale & Zuiderveen Borgesius, 2021, para. 9), but ignores some of the most troubling current applications. An example of this is emotion recognition systems (see McStay, 2016, 2020; Hacker, 2022). Paradoxically, there seems to be too much future and too little present in Art. 5 AIA.

High-risk AI systems: The overwhelming majority of rules in the AIA are dedicated to high-risk applications (Art. 6 et seqq. AIA). They cover a broad spectrum of the techniques of temporalisation. In this, the AIA attempts to be specific, focusing on temporality by direct regulation and reviews, rather than the potentially vaguer temporal interpretation.

Smart city AI as high-risk AI?: In the smart city context, however, such rules only unfold their potential if machine learning used in the smart city qualifies as a high-risk application. These are defined, for our purposes, in Annex III AIA. In fact, many smart city AI systems may be considered high-risk, including systems: based on biometrics, such as face recognition systems; as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity; for education and vocational training; for essential services such as public assistance benefits or emergency response services; and for specific law enforcement purposes, such as profiling potential offenders in the course of criminal investigations. Annex III hence covers a wide range of potential smart city applications of AI.

However, two shortcomings remain. First, in many cases, an additional significant risk to fundamental rights must be shown for the AIA high-risk rules to apply (Art. 6(3) AIA). This may pose a specific problem if private actors use AI applications – traditionally, only the state is bound by fundamental rights, not private actors.[6] Furthermore, risks may not be deemed significant enough for the time. The second

6. Cf. Art. 51(1) Charter of Fundamental Rights; CJEU, Case 414/16, Egenberger; Lenaerts, 2019, p. 788 et seqq.

gap is evident from the smart streetlight example and directly relates to temporality: smart city tools may not initially have been conceived of to serve a high-risk purpose. The streetlights in San Diego were supposed to collect traffic and environmental data (Marx, 2020) and, even if they used AI for it, would not have qualified as high-risk in an EU setting. In principle, only the function creep toward law enforcement might trigger the application of the high-risk rules. However, access to the streetlight data would have to cross the threshold of "profiling", which implies automated processing.[7] This is at least highly dubious if human law enforcement agents analyse only a single video stream.

Ultimately, to acknowledge their supreme importance to fundamental rights and reduce legal uncertainty, smart city AI applications should, in our opinion, generally qualify as high-risk. Annex III AIA should be updated accordingly (see also below: Legislative temporality review)

Forward-looking regulation: The streetlights case is the epitome of function creep. In the AIA, such use for additional purposes is addressed in one of the prime examples of forward-looking regulation: Art. 4a-4c AIA, which deals with general-purpose AI systems (GPAIS) (see, e.g., Hacker, Engel & Mauer, 2023). The provisions were only added during the late drafting stage. While the general thrust of including GPAIS should be welcomed, the concrete implementation remains problematic. GPAIS are defined in Art. 3(1b) AIA as systems that "may be used in a plurality of contexts and [read: or] be integrated in a plurality of other AI systems". Under Art. 4b AIA, if GPAIS may be used as high-risk AI applications, they must conform to the core rules governing such systems under the AIA, i.e., the obligations regarding a risk management system (Art. 9 AIA); the training data quality (Art. 10 AIA); the technical documentation (Art. 11 AIA); the transparency and the performance quality provisions (Art. 13 and 15 AIA) (on these, in particular, see Veale & Zuiderveen Borgesius, 2021; Ebers et al., 2021; Hacker & Passoth, 2022). Hence, the law compels developers to take possible future uses and concomitant risks into account when designing systems which may be used in such contexts.

The main problem with this approach is that GPAIS, which has generally been considered the future of AI (Han et al., 2021), may be used for a wide range of different purposes. Drawing up a risk management system for such encompassing and powerful systems borders on the impossible (Hacker, 2022a, p. 14). Therefore, it would be better if the entity seeking to use GPAIS for concrete high-risk applications was compelled to comply with the respective high-risk obligations, not the

7. Art. 3(4) LED, cf. Annex III point 6(f) AIA.

GPAIS provider. Furthermore, many GPAIS systems are provided open source or for free (for example, TensorFlow; GPT-NeoX; ChatGPT). It remains doubtful whether open source projects can handle the administrative costs and burden of complying with the AI Act. Again, focusing on the high-risk user, instead of the GPAIS provider, would solve that problem.

Both the current version of Art. 4b AI Act and the proposal just mentioned provide redress in our streetlight example. If a non-negligible risk exists: law enforcement agencies will legally use AI systems for any acts listed in Annex III point 6 (e.g., profiling or prediction), and they must comply with the essential high-risk rules. As said, it would be more straightforward to oblige the law enforcement agency to bring the GPAIS in conformity with the AI Act, rather than the streetlamp manufacturer, for example. Again, however, the same threshold for profiling discussed above applies. In our view, Art. 4b AIA, therefore, expands the scope of high-risk applications to all AI systems to which law enforcement agencies could legally, under the respective laws of any of the EU Member States, have access to perform acts listed under Annex III point 6 AIA; this may still not be sufficient enough to take less comprehensive but still sensitive access into account.[8] This provides yet another argument for including all smart city applications under the heading of high-risk AI.

Significantly, Art. 4b AIA arguably covers the mere collection of data for a machine learning training data set, as discussed in our FRT entry example. At first blush, one might doubt whether a mere data set constitutes a (general-purpose) AI *system*, as it cannot perform any AI-specific tasks on its own. However, it is a core component of AI systems and may be integrated into those (cf. also Recital 12aa AIA). Therefore, in our view, it qualifies as a GPAIS and developers of data sets intended for use in AI systems must comply with the training data regime in Art. 10 AIA.[9] However, the rules of Art. 10 AI Act need to be adapted to generic training data sets, as opposed to those for concrete use cases. Indeed, the Commission will likely have the power to adopt implementing acts to this effect (Art 4b(1) AI Act). This would effectively close the loophole left by the disapplication of non-discrimination law and arguably strike a fair balance: it subjects the developers to the more specific duties of Art. 4b(1), 10 AIA, with corresponding obligations to assemble a data set that is, to the extent possible, relevant, representative, free of errors

8. Any provider disclaimer to the contrary would probably be invalid, Art. 4c(2) AIA (Hacker, Engel & Mauer, 2023).

9. Note that this may change in the final version of the AI Act and is currently under discussion by the European Parliament.

and complete. It does spare them the strict liability of non-discrimination law for somewhat hypothetical use cases down the ML pipeline.

Other provisions in the AIA equally seek to hedge specific future risks. Art. 10 AIA, as mentioned, attempts to prevent the perpetuation of biases and errors in data sets in future decision making. More specifically, the training data needs to be relevant with respect to the envisioned task. This criterion should be interpreted to include the timeliness of training data (Hacker, 2021, p. 297); thus, outdated data sets may not be used anymore for training purposes, directly tackling temporality. If personal data are used, this is equally implied by Art. 5(1)(d) GDPR (Hacker, 2021, pp. 284-285). Such rules attempt to guard against the risk of AI becoming unfit and increasingly opaque, to future users and affected persons (cf. also Delacroix, 2022). In turn, Art. 15(3) AIA ensures that online learning systems are equipped with proper safeguards against the development of biassed outcomes. This is clearly modelled on the ML bot, which started using racial slurs shortly after activation (Schwartz, 2019). And finally, the provisions on regulatory sandboxes (Art. 53 et seqq. AIA) seek to establish an environment in which risk-prone applications may be tested under real but controlled conditions (for a methodological critique, see Ranchordás, 2021).

Overall, the AIA establishes a nuanced regime of forward-looking regulation, particularly with the provision of general-purpose AI systems.

Adaptive regulation: Like the GDPR, the AIA, in theory, follows a risk-based approach as a strategy for adaptive regulation (Recital 14 AIA). However, its application and impact are hamstrung by the essentially binary character of its regulatory structure: either an AI system qualifies as high-risk and is thoroughly regulated, with temporalising elements, or it is not, leaving it essentially unregulated. Therefore, there is a clear need for the application of a risk-based framework also *within* the category of high-risk AI applications – in other words, the AI Act needs a more nuanced scale of compliance obligations within the high-risk AI category. This implies that the stringency of rules which cover all high-risk applications, such as the regime of training data or the performance requirements, must be adapted to the specific risk the AI application poses, including potential shifts in purpose (cf. Art. 4b AIA). In our view, for example, an application intended or prone to be used by law enforcement personnel should be vetted even more rigorously than a system designed for recruitment, despite both being instantiations of high-risk systems (cf. Annex III AIA). Since smart city applications have the potential to significantly impact fundamental rights (e.g., data protection, non-discrimination, assembly), basic necessities and participation in public life, a particularly demanding standard

should be applied.

Compliance temporality review: Forward-looking and adaptive regulation are examples of temporality by direct regulation, which specifically address concrete technologies or risks. The AIA combines this with a strategy of temporality by review. Art. 9(1) AIA requires the instalment of a risk management system for high-risk AI. Providers need to engage in continuous and iterative testing for known *and foreseeable* errors and biases. Similarly, in 2022 the Algorithmic Accountability Act (AAA), introduced (but stalled) in the U.S. Congress, would require covered companies to test AI systems continuously (Sec. 4(a)(4) AAA). For example, testing for discrimination concerning traditionally protected attributes (e.g., sex, gender, ethnicity), but also novel attributes such as socioeconomic status. Again, the orientation of both provisions towards the future is evident: Art. 9 AIA and Sec. 4(a)(3)(C) AAA force the person responsible for compliance to engage in recurrent reviews and to forecast poor performance (compliance temporality review). Finally, under the AIA, professional users need to continuously monitor the active deployment of the system and watch out for specific risks (Art. 29(4) AIA).

Legislative temporality review: Finally, according to Art. 84 AIA, the definition of AI and the list of high-risk applications, as well as the entire AIA, must be evaluated and potentially adapted by EU legislators every 2 to 4 years, respectively. This amounts to a legislative temporality review: the legislators are called upon to optimise institutional learning (see Armstrong, Gorst & Rae, 2019; Dimitropoulos & Hacker, 2016) and to refine the AIA over time. Arguably, one of the most important points for future review is to close the gaps identified in the high-risk rule context (delete the additional fundamental rights requirement in Art. 6(3) AIA; ensure the applicability of the AIA to function creep). Given the potential of smart city applications for surveillance and discrimination, and their overall importance for participation in public life and public discourse, we affirm our suggestion to include smart city AI applications in the category of high-risk AI applications.

Section 3: Converging temporalities between law and politics?

The preceding parts have argued that, on the one hand, several instruments may be harnessed in politics and the law to cope with the phenomenon of temporality and to implement substantial smartness in smart cities, based on participation and respect for human rights. On the other hand, the discussion has shown that frictions and challenges still abound. For space constraints, we can only scratch the surface of possible solutions. The last part nevertheless seeks to combine insights

from the two fields to mitigate some of these pressing issues. In this way, politics and law may mutually reinforce one another: the law can foster and safeguard participation and political action may highlight and strengthen human and fundamental rights.

Fostering participation: Inclusive AI processes

Participatory smartness requires the motivation, but also the ability of citizens to make their voices heard within the confines of content moderation rules such as the DSA. In this endeavour, intelligent legal design may help. Both the GDPR and the AIA do not excel in offering avenues of participation for affected persons before or during data processing (cf. Art. 35(9) GDPR) or AI deployment (cf. Recitals 76 and 81 AIA; Art. 56(3) and 59(2-3) AIA). Smart city regulation and technology law may more broadly draw inspiration from two US initiatives: the proposed Algorithmic Accountability Bill (AAB), which was presented in a public hearing in Washington's state legislature in early 2022 (Kaminski, 2023, pp. 66-67), and the proposal for a federal AAA (see above, Compliance temporality review). The AAB requires direct consultation with the representatives of disproportionately impacted communities during the AI rulemaking process (Sec. 3 AAB), and it mandates the publication of an algorithmic accountability report, which the public may comment upon for at least 30 days (Sec. 5(3) AAB). In a similar vein, the AAA would require covered entities to consult, to the extent possible, with external stakeholders while conducting an AI impact assessment (Sec. 3(a)(1)(G) AAA). In our view, if such *ex-ante* involvement were legally required and digitally implemented in the context of smart cities, transparency toward the public, good governance and participatory smartness would benefit substantially (cf. also Metcalf et al., 2021, p. 743; Kaminski, 2023, p. 79). The law, in this sense, would pave the way for participation.

An even more ambitious format would involve stakeholders directly in the design of the smart city AI system, for example in the choice of the training data, the model type or the explanations (Delacroix, 2022, pp. 12-13; Hacker & Passoth, 2022, pp. 366-367). Co-design strategies can be fruitfully applied in this context (Hacker & Passoth, 2022, pp. 366-367), but again need to be backed up by legal obligations to ensure their application and smooth performance.

Protecting politics: Safeguarding local citizen platforms to safeguard human rights

Participation, moreover, only functions if all voices can be heard. While local citizen platforms are promising tools in this endeavour, they are also plagued by hate speech, abuse and other shortcomings. As mentioned, the EU has recently passed

the Digital Services Act (DSA), which is supposed to address these issues. As seen, it features novel instruments such as trusted flaggers, compulsory content moderation systems (including dispute resolution mechanisms), transparency obligations for platforms, fundamental rights impact assessments and other tools to foster safer digital environments. Some of the instruments mirror the AIA, such as risk management systems and independent audits. We cannot offer an in-depth analysis and critique of the DSA here. Suffice it to say that for local citizen platforms to function appropriately and redeem their promise to give (approximately) equal voice to all affected persons, legal intervention is necessary (Echikson & Knodt, 2018; Pielemeier, 2020). Regulation needs to safeguard local citizen platforms, both to ensure adherence to human rights norms within the platforms and facilitate the active exercise of human rights through and on the platforms themselves.

Local enforcement with EU-wide impact

The third area of interdisciplinary convergence, arguably, is enforcement. By nature, enforcement contains a strong forward-looking element by calibrating the level of deterrence and thus steering future actions (Becker, 1968; Posner, 1985). In smart city contexts, more specifically, a recent landmark decision of the CJEU harbours the potential to spur local enforcement of GDPR breaches. In April 2022, the Court ruled in Meta vs vzbv that consumer associations can sue data controllers for violations of the GDPR (Case C-319/20, para. 83). This brings local action to the forefront: citizen groups or local watchdogs may monitor smart city applications and team up with existing, or form novel, consumer protection associations to effectively bring cases, potentially up to the CJEU (Art. 80(2) GDPR). If one assumes that discriminatory data practices violate the GDPR principle of fair data processing (Article 29 Data Protection Working Party, 2018, p. 10; Hacker, 2018, p. 1172), the same strategy can be pursued to combat discrimination in the smart city. In short, data protection or consumer protection associations formed on the local level are now endowed with an EU-wide impact. The approach, however, does not work for the AIA since that regulation does not confer any subjective rights to natural persons or associations.

Political human rights activism

The AIA is an area where local action and decentralised enforcement must take a different form. Here, political activism and local citizen platforms are required to flag problems, misconceptions and abuse of AI systems in the smart city context. The political discourse engendered by these means needs to ensure that the deficiencies in the design and implementation of the AIA (see, e.g., Veale &

Zuiderveen Borgesius, 2021) are appropriately highlighted in the smart city context and beyond.

Ultimately, therefore, the law can help politics by establishing mandates and safeguards for digital participation and by enabling local action to rise to the top judicial levels. Conversely, politics is called upon to assist the law where the latter fails to provide affected persons with effective mechanisms to participate in the design of a law, challenge its implementation, react to novel risks, or invoke their human and fundamental rights. In this way, the gap between the pace of technological change and the steadfastness of the law may be reduced by a combination of politics and the law, which simultaneously contributes to making future urban spaces not only formally, but also substantially, smart.

Conclusion

In this paper, we have shown that the double challenge of (1) ensuring effective human and fundamental rights protection in smart cities and of (2) temporalising how legal provisions can be met by a strategy which we have termed "substantive smartness". The concept distinguishes between two dimensions: law-immanent (= HR-respecting) smartness and law-external (= participatory) smartness. Law-immanent smartness safeguards human or fundamental rights by regulatory means in the smart city, while simultaneously and adaptively accommodating technological change. Different strategies can be mobilised to these ends within legal regimes such as the DSA, the GDPR, non-discrimination law or the proposed AI Act: temporality by direct regulation, by interpretation and by review.

Law-external smartness refers to the mobilisation of those local social contexts in which the implementation of technological innovations is directly experienced and can be shaped by participation. Supportive but critical political mobilisation is preconditional but not utopian. A close link between digital innovations and civic participation can ensure critical monitoring of the implementation process, and thus meet the challenge of the necessary temporality of law by strengthening democratic procedures.

Law and politics are closely intertwined in any strategy that fosters substantive smartness. Law provides the instruments necessary for tying smart city practices to fundamental rights and for mandating and safeguarding civic participation; politics guarantees that local society itself couples regulations to fundamental and human rights, thus linking substantial smartness to the democratic process. The concept of substantial smartness applies not only to smart cities, but more broadly

to the governance of AI systems and technology in a variety of settings in which they interact with the general public or specific individuals. Examples may include credit scoring, people analytics and use of AI systems by administrative bodies. Participatory strategies, not envisioned in the AI Act, should complement current regulatory efforts to build legitimacy for and trust in AI systems, in smart cities and beyond (see also Hacker & Passoth, 2022, pp. 366-367).

References

Aldewereld, H., Dignum, V., & Tan, Y. (2015). Design for values in software development. In J. van den Hoven, P. E. Vermaas, & I. van de Poel (Eds.), *Handbook of ethics, values, and technological design* (pp. 831–845). Springer Netherlands. https://doi.org/10.1007/978-94-007-6970-0_26

Amin, K. (2014). Temporality. *TSQ: Transgender Studies Quarterly*, *1*(1–2), 219–222. https://doi.org/10.1215/23289252-2400073

Armstrong, H., Gorst, C., & Rae, J. (2019). *Renewing regulation. 'Anticipatory regulation' in an age of disruption* [Report]. Nesta. https://media.nesta.org.uk/documents/Renewing_regulation_v3.pdf

Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data, WP 136* (01248/07/EN WP 136). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Data Protection Working Party. (2012a). *Opinion 02/2012 on facial recognition in online and mobile services, WP 192* (00727/12/EN WP 192). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Article 29 Data Protection Working Party. (2012b). *Opinion 3/2012 on developments in biometric technologies, WP 193* (18/EN WP266). https://ec.europa.eu/newsroom/article29/redirection/document/51517

Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on anonymisation techniques, WP216* (0829/14/EN WP216). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Data Protection Working Party. (2018). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (17/EN WP251rev.01). https://ec.europa.eu/newsroom/article29/redirection/document/49826

Artyushina, A., & Wernick, A. (2021, November 8). Smart city in a post-pandemic world: Small-scale, green, and over-policed. *Spacing*. https://spacing.ca/toronto/2021/11/08/smart-city-tech-post-pandemic-small-scale-green-over-policed/

Atik, J., & Jeutner, V. (2021). Quantum computing and computational law. *Law, Innovation and Technology*, *13*(2), 302–324. https://doi.org/10.1080/17579961.2021.1977216

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169–217. https://doi.org/10.1086/259394

Bennett Moses, L. (2007). Recurring dilemmas: The law's race to keep up with technological change.

SSRN Electronic Journal. https://doi.org/10.2139/ssrn.979861

Bennett Moses, L. (2016). *Regulating in the face of sociotechnical change* (R. Brownsword, E. Scotford, & K. Yeung, Eds.; Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199680832.013.49

Black, J. (2005). The emergence of risk-based regulation and the new public risk management in the United Kingdom. *Public Law*, *Autumn*, 512–549. http://eprints.lse.ac.uk/id/eprint/15809

Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation: REALLY RESPONSIVE RISK. *Law & Policy*, *32*(2), 181–213. https://doi.org/10.1111/j.1467-9930.2010.00318.x

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, *81*, 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

Burbank, S. B., Farhang, S., & Kritzer, H. M. (2013). Private enforcement. *Lewis & Clark Law Review*, *17*(3), 637–722. https://scholarship.law.upenn.edu/faculty_scholarship/488

Camero, A., & Alba, E. (2019). Smart city and information technology: A review. *Cities*, *93*, 84–94. https://doi.org/10.1016/j.cities.2019.04.014

Capdevila, I., & Zarlenga, M. I. (2015). Smart city or smart citizens? The Barcelona case. *Journal of Strategy and Management*, *8*(3), 266–282. https://doi.org/10.1108/JSMA-03-2015-0030

Carr, C., & Hesse, M. (2020). When Alphabet Inc. plans Toronto's waterfront: New post-political modes of urban governance. *Urban Planning*, *5*(1), 69–83. https://doi.org/10.17645/up.v5i1.2519

Cavazos, J. G., Phillips, P. J., Castillo, C. D., & O'Toole, A. J. (2021). Accuracy comparison across face recognition algorithms: Where are we on measuring race bias? *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(1), 101–111. https://doi.org/10.1109/TBIOM.2020.3027269

Charnock, G., March, H., & Ribera-Fumaz, R. (2021). From smart to rebel city? Worlding, provincialising and the Barcelona Model. *Urban Studies*, *58*(3), 581–600. https://doi.org/10.1177/0042098019872119

Clifford, D., & Ausloos, J. (2018). Data protection and the role of fairness. *Yearbook of European Law*, *37*, 130–187. https://doi.org/10.1093/yel/yey004

Colomb, C., & Novy, J. (Eds.). (2016). *Protest and resistance in the tourist city*. Routledge.

Council of the European Union. (2022). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts — General approach, Interinstitutional File: 2021/0106(COD), Doc. 14954/22*.

Dawson, P., & Sykes, C. (2019). Concepts of time and temporality in the storytelling and sensemaking literatures: A review and critique. *International Journal of Management Reviews*, *21*(1), 97–114. https://doi.org/10.1111/ijmr.12178

Delacroix, S. (2022). Diachronic interpretability and machine learning systems. *Journal of Cross-Disciplinary Research in Computational Law*, *1*(2). https://journalcrcl.org/crcl/article/view/9

Dimitropoulos, G., & Hacker, P. (2016). Learning and the law: Improving behavioral regulation from an international and comparative perspective. *Journal of Law and Policy*, *25*(2), 473–548. https://brooklynworks.brooklaw.edu/jlp/vol25/iss2/10

Donahoe, E., & Metzger, M. M. (2019). Artificial intelligence and human rights. *Journal of Democracy*, *30*(2), 115–126. https://doi.org/10.1353/jod.2019.0029

Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). The European Commission's Proposal for an Artificial Intelligence Act — A critical assessment by members of the Robotics and AI Law Society (RAILS). *J*, *4*(4), 589–603. https://doi.org/10.3390/j4040043

Echikson, W., & Knodt, O. (2018). *Germany's NetzDG: A key test for combatting online hate* (Research Report No. 2918/09). Centre for European Policy Studies. http://aei.pitt.edu/id/eprint/95110

Eckhoff, D., & Wagner, I. (2018). Privacy in the smart city — Applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 489–516. https://doi.org/10.1109/COMST.2017.2748998

Edwards, L. (2016). Privacy, security and data protection in smart cities: *European Data Protection Law Review*, *2*(1), 28–58. https://doi.org/10.21552/EDPL/2016/1/6

COMMISSION IMPLEMENTING DECISION amending Implementing Decision C(2021)1940 final on the adoption of the work programme for 2021-2022 within the framework of the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation and on its financing, as regards Missions, no. C(2021)9128 (202 C.E.). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282021%299128

European Data Protection Board (EDPB). (2022). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (Guidelines 05/2022 Version 1.0). European Data Protection Board. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

Fairfield, J. A. T. (2021). *Runaway technology: Can law keep up?* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781108545839

Finch, K., & Tene, O. (2013). Welcome to the metropticon: Protecting privacy in a hyperconnected town. *Fordham Urban Law Journal*, *41*(5), 1581–1615. https://ir.lawnet.fordham.edu/ulj/vol41/iss5/4

Finck, M., & Pallas, F. (2020). They who must not be identified — Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Flak, L. S., & Hofmann, S. (2020). The impact of smart city initiatives on human rights. *Proceedings of Ongoing Research, Practitioners, Posters, Workshops, and Projects at EGOV-CeDEM-EPart 2020*, *2797*. https://ceur-ws.org/Vol-2797/paper16.pdf

Foster, K. R., Vecchia, P., & Repacholi, M. H. (2000). Science and the precautionary principle. *Science*, *288*(5468), 979–981. https://doi.org/10.1126/science.288.5468.979

Garfinkel, S. L., & Hoofnagle, C. J. (2022). *ACM TechBrief: Quantum computing and simulation*. ACM. https://doi.org/10.1145/3551664

Gellert, R. (2015). Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, *5*(1), 3–19. https://doi.org/10.1093/idpl/ipu035

Goodman, E. P. (2019). Smart city ethics: The challenge to democratic governance – [Draft chapter for Oxford handbook of the ethics of artificial intelligence]. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3391388

Graham, S., & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy*, *23*(2), 227–248. https://doi.org/10.1177/0261018303023002006

Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, *55*(Issue 4), 1143–1185. https://doi.org/10.54648/COLA2018095

Hacker, P. (2020). *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB [Data privacy law: New technologies in the area of conflict between data protection law and the German Civil Code (BGB)]*. Mohr Siebeck.

Hacker, P. (2021a). A legal framework for AI training data — From first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, *13*(2), 257–301. https://doi.org/10.1080/17579961.2021.1977219

Hacker, P. (2021b). Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal*, eulj.12389. https://doi.org/10.1111/eulj.12389

Hacker, P. (2023). *The European AI Liability Directives — Critique of a half-hearted approach and lessons for the future* (arXiv:2211.13960). arXiv. http://arxiv.org/abs/2211.13960

Hacker, P., Engel, A., & Mauer, M. (2023). *Regulating ChatGPT and other large generative AI models* (arXiv:2302.02337). arXiv. http://arxiv.org/abs/2302.02337

Hacker, P., & Passoth, J.-H. (2022). Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond. In A. Holzinger, R. Goebel, R. Fong, T. Moon, K.-R. Müller, & W. Samek (Eds.), *XxAI - Beyond explainable AI* (Vol. 13200, pp. 343–373). Springer International Publishing. https://doi.org/10.1007/978-3-031-04083-2_17

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Wimmersperg, U. (2000, September 28). *The vision of a smart city*. 2nd International Life Extension Technology Workshop, Paris. https://www.osti.gov/biblio/773961

Han, X., Zhang, Z., Ding, N., Gu, Y., Liu, X., Huo, Y., Qiu, J., Yao, Y., Zhang, A., Zhang, L., Han, W., Huang, M., Jin, Q., Lan, Y., Liu, Y., Liu, Z., Lu, Z., Qiu, X., Song, R., … Zhu, J. (2021). Pre-trained models: Past, present and future. *AI Open*, *2*, 225–250. https://doi.org/10.1016/j.aiopen.2021.08.002

Hankin, C. (2022). *ACM TechBrief: Smart cities*. ACM. https://doi.org/10.1145/3534515

Hayek, F. A. (1945). The use of knowledge in society. *The American Economic Review*, *35*(4), 519–530. https://www.jstor.org/stable/1809376

High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI* [Report]. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Howells, G., Twigg-Flesner, C., & Willett, C. (2017). Product liability and digital products. In T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (Eds.), *EU Internet Law* (pp. 183–195). Springer International Publishing. https://doi.org/10.1007/978-3-319-64955-9_8

Information Commissioner's Office. (2021). *The use of live facial recognition technology in public places* [Opinion]. https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Ingold, T. (1993). The temporality of the landscape. *World Archaeology*, *25*(2), 152–174. https://doi.o

rg/10.1080/00438243.1993.9980235

Jaszczolt, K. M. (2009). *Representing time: An essay on temporality as modality*. Oxford University Press. https://www.jstor.org/stable/23315136

Kaminski, M. E. (2022). Regulating the risks of AI. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4195066

Kempin Reuter, T. (2020). *Smart city visions and human Rights: Do they go together?* (No. 2020–006; Carr Center Discussion Paper Series). Harvard Kennedy School. https://carrcenter.hks.harvard.edu/publications/smart-city-visions-and-human-rights-do-they-go-together

Khan, L. A. (2009). Temporality of law. *McGeorge Law Review*, *40*(1), 55–106. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/4

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security* (Government Data Forum). Data Protection Unit, Department of the Taoiseach. https://mural.maynoothuniversity.ie/7242/1/Smart

Koops, B.-J. (2021). The concept of function creep. *Law, Innovation and Technology*, *13*(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

Kroll, J. A. (2022). *ACM TechBrief: Facial recognition*. ACM. https://doi.org/10.1145/3520137

Landes, W. M., & Posner, R. A. (1975). The private enforcement of law. *The Journal of Legal Studies*, *4*(1), 1–46. https://doi.org/10.1086/467524

Lenaerts, K. (2019). Limits on limitations: The essence of fundamental rights in the EU. *German Law Journal*, *20*(6), 779–793. https://doi.org/10.1017/glj.2019.62

Liegl, M., Oliphant, R., & Buscher, M. (2015, May). Ethically aware IT design for emergency response: From co-design to ELSI co-design. *Proceedings of the ISCRAM 2015 Conference*. International Conference on Information Systems for Crisis Response and Management, Kristiansand. http://idl.iscram.org/files/michaelliegl/2015/1202_MichaelLiegl_etal2015.pdf

Lynskey, O. (2015). *The foundations of EU data protection law*.

March, H., & Ribera-Fumaz, R. (2016). Smart contradictions: The politics of making Barcelona a self-sufficient city. *European Urban and Regional Studies*, *23*(4), 816–830. https://doi.org/10.1177/0969776414554488

Martin, G. E. (2017). Those closest to the problem are closest to the solution. *The Appeal*. https://theappeal.org/those-closest-to-the-problem-are-closest-to-the-solution-555e04317b79/

Marx, J. (2020). Police used smart streetlight footage to investigate protesters. *Voice of San Diego*. https://voiceofsandiego.org/2020/06/29/police-used-smart-streetlight-footage-to-investigate-protesters/

McStay, A. (2016). Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy). *Big Data & Society*, *3*(2). https://doi.org/10.1177/2053951716666868

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society*, *7*(1). https://doi.org/10.1177/2053951720904386

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: A review of the literature on smart urban governance. *International Review of Administrative Sciences*, *82*(2), 392–408. https://doi.org/10.1177/0020852314564308

Metcalf, J., Moss, E., Watkins, E. A., Singh, R., & Elish, M. C. (2021). Algorithmic impact assessments and accountability: The co-construction of impacts. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 735–746. https://doi.org/10.1145/3442188.3445935

Neyer, J., & Worschech, S. (2022, August). *Pragmatic smartness. technology, local governance and the promise of better democracy*. ECPR General Conference, Innsbruck.

O'Brien, T. C., Tyler, T. R., & Meares, T. L. (2020). Building popular legitimacy with reconciliatory gestures and participation: A community-level model of authority. *Regulation & Governance*, *14*(4), 821–839. https://doi.org/10.1111/rego.12264

Pielemeier, J. (2020). *Disentangling disinformation: What makes regulating disinformation so difficult?* https://doi.org/10.26054/0D-CJBV-FTGJ

Posner, R. A. (1985). An economic theory of the criminal law. *Columbia Law Review*, *85*(6), 1193–1231. https://doi.org/10.2307/1122392

Ranchordás, S. (2021). Experimental regulations and regulatory sandboxes – Law without order?: Special issue experimental legislation in times of crisis, Sofia Ranchordás & Bart van Klink (eds.). *Law and method*. https://doi.org/10.5553/REM/.000064

Robinson, J. P., Livitz, G., Henon, Y., Qin, C., Fu, Y., & Timoner, S. (2020). Face recognition: Too bias, or not too bias? *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*. https://doi.org/10.1109/CVPRW50498.2020.00008

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, *10*(1), 3069. https://doi.org/10.1038/s41467-019-10933-3

Sadowski, J., & Pasquale, F. (2015). The spectrum of control: A social theory of the smart city. *First Monday*. https://doi.org/10.5210/fm.v20i7.5903

Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. *Neue Juristische Wochenschrift: NJW*, *69*(26), 1841–1847.

Schwartz, O. (2019, November 25). In 2016, Microsoft's racist chatbot revealed the dangers of online conversation. *IEEE Spectrum*. https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation

Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation. *EMBO Reports*, *20*(6). https://doi.org/10.15252/embr.201948316

Shavell, S. (1984). Liability for harm versus regulation of safety. *The Journal of Legal Studies*, *13*(2), 357–374. https://doi.org/10.1086/467745

Smith, A., & Martín, P. P. (2021). Going beyond the smart city? Implementing technopolitical platforms for urban democracy in Madrid and Barcelona. *Journal of Urban Technology*, *28*(1–2), 311–330. https://doi.org/10.1080/10630732.2020.1786337

Tan, H., & Chung, I. (2020). Secure authentication and key management with blockchain in VANETs. *IEEE Access*, *8*, 2482–2498. https://doi.org/10.1109/ACCESS.2019.2962387

Tryfonidou, A. (2020). Case C-507/18 NH v Associazione Avvocatura per i diritti LGBTI – Rete Lenford: Homophobic speech and EU anti-discrimination law. *Maastricht Journal of European and Comparative Law*, *27*(4), 513–521. https://doi.org/10.1177/1023263X20946535

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Wachter, Sandra; (2020). *Affinity profiling and discrimination by association in online behavioral advertising*. https://doi.org/10.15779/Z38JS9H82M

Wlodarczak, P. (2017). Smart cities – Enabling technologies for future living. In A. Karakitsiou, A. Migdalas, S. Th. Rassia, & P. M. Pardalos (Eds.), *City networks* (Vol. 128, pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-319-65338-9_1

Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137–155. https://doi.org/10.1111/rego.12401

Yeung, K., Howes, A., & Pogrebna, G. (2020). AI governance by human rights-centered design, deliberation, and oversight: An end to ethics washing. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford handbook of ethics of AI* (pp. 75–106). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*(10), 1572–1593. https://doi.org/10.1080/13642987.2020.1743976

Zuiderveen Borgesius, F. J., Trilling, D., Möller, J., Bodó, B., de Vreese, C. H., & Helberger, N. (2016). Should we worry about filter bubbles? *Internet Policy Review*, *5*(1). https://doi.org/10.14763/2016.1.401

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

cnrs centre internet et societe

University of Tartu Johan Skytte Institute of Political Studies