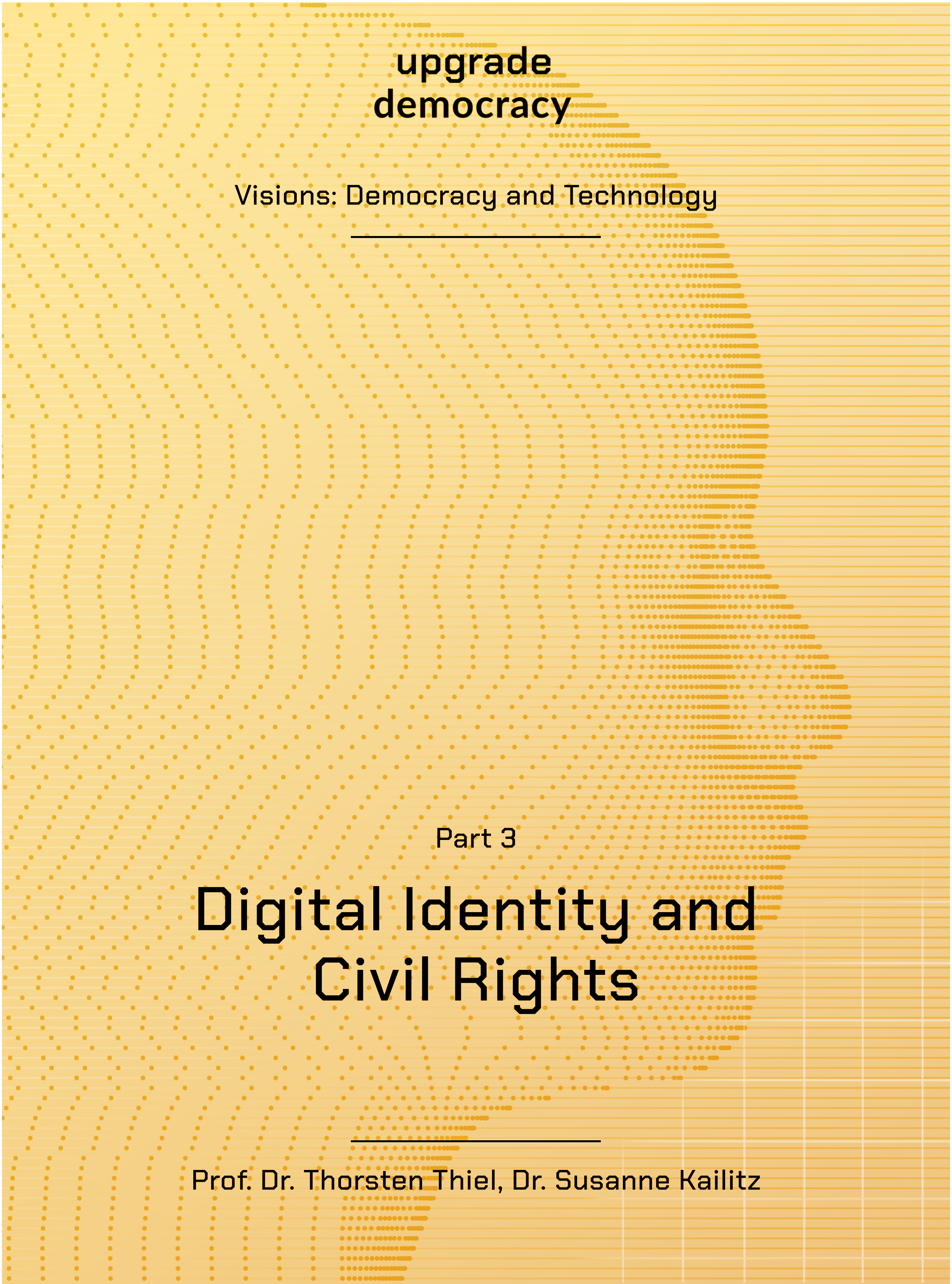

upgrade
democracy

Visions: Democracy and Technology

Part 3

Digital Identity and Civil Rights

Prof. Dr. Thorsten Thiel, Dr. Susanne Kailitz

BertelsmannStiftung

In 1993, the American magazine The New Yorker published a cartoon featuring two dogs sitting in front of a computer. One dog says to the other, “On the Internet, nobody knows you’re a dog.” This now-famous meme still symbolises, for many, the relationship between communication and identity in the digital realm. However, much has changed since 1993. The questions of whether we surf the internet under the protection of anonymity or whether we can prove that we are who we claim to be have become increasingly important. Identification and anonymisation in digital contexts also play a significantly more crucial role politically and economically. This development is expected to remain dynamic – and it has implications for democracy, which we aim to explore here.

What is it about?

Developments in the field of digital identity are complex. This is partly because, while anonymity in digital communication has indeed decreased, no overarching standards for digital identity have yet been established. We, therefore, anticipate further attempts to establish identification procedures and identity management for digital communication. Three types of identification systems are particularly significant: state, private sector, and decentralised systems.

State Identification and Authentication Procedures

As public administration becomes more digitalised and electronic processes for citizen participation are expanded, the development and extension of state procedures for certifying digital identities are being promoted. A unified and comprehensive identification procedure is intended to significantly accelerate and improve societal and political processes (ranging from filing tax returns and registering a car to electronic health records). Democratic states are also striving to make secure and data protection-compliant identification possible. Despite all efforts, however, the acceptance of the various available technologies among the German population remains relatively low. This is less due to technical obstacles and more to the fact that these technologies usually only offer isolated options for action. In other countries, overarching state identity systems have become more established: partly due to their high functionality (Denmark, Estonia) and partly due to a strong obligatory nature (such as the Indian Aadhaar system). Another area where state digital identity procedures are increasingly being tested is the area of immigration and migration. There seems to be a greater willingness to experiment with new methods and to set aside concerns in dealing with foreigners than with one's own citizens. Thus, a testing ground for a variety of identity and identification procedures is emerging here.

Private Sector Identification and Authentication Procedures

The attribution of digital identity has also gained significant traction in commercial contexts over many years. Fixed and recurrently identifiable digital identities are of enormous value in a data-centred economy, as they allow for the tailoring of services and offers or the personalisation of advertising. Two major trends can be observed in the area of economic identification procedures: Firstly, isolated identity systems – where users identify themselves with a single service or provider – are increasingly being replaced by federated identity procedures, in which identities can be used across many services (such as the identity management systems of Google and Apple). This trend is further strengthened by so-called digital wallets, systems that combine multiple digital identities and make them usable together. Secondly, major platforms are becoming increasingly adept at assigning identity based on a wide range of observation points, allowing them to categorise actions and behaviours online even without explicit identification.

Decentralised Identification and Authentication Procedures

A third developmental direction we observe involves identity management systems that are more decentralised, often referred to as Self-Sovereign Identity in the academic literature. These systems are often, though not necessarily, associated with discourses surrounding blockchain. This type of identity management is characterised by the attempt to develop technical solutions where the identity verification is not carried out by a state or commercial entity but is instead created by a network of verification agents. Furthermore, the focus here is more on anonymous or pseudonymous actions. When using blockchain, the proof of work implementation – where cryptographic tasks must be solved with great computational effort – is particularly criticised due to its enormous energy consumption. So-called proof of stake systems, where the verification agents deposit a kind of collateral, are currently still not reliable enough and must still credibly demonstrate their lower energy requirements.

Fingerprint, Facial Recognition, or Iris Scan – The Trend Towards Biometrics

Across all three of these developmental directions, the importance and use of biometric identification procedures are increasing significantly. Here, identification and verification are carried out using biological characteristics that have a high uniqueness. This is intended to protect users from identity theft while also making the application faster and more convenient by eliminating the need for passwords. Due to the increasing penetration of public spaces with sensors, it is expected that these biometric identification procedures, after a phase of scrutiny, have relatively good chances of becoming widely used and employed in various contexts. The key issue will be how digital identities and biometric identification procedures are perceived, whether they are considered secure, and which actors under which circumstances gain access to identification capabilities. However, it is also clear that the more biometric data is used for identification, the greater the risk of identity theft, as the data is often stored in a decentralised manner and is based on non-exchangeable characteristics.

What are the Potential and Risks?

Identification procedures are often indispensable for political processes. Only through the determination of identity can action opportunities be fairly distributed and assigned, and services made accessible. This applies to casting a vote in an election just as it does to receiving social benefits or taxing income and wealth. The state must be certain and ensure that it is dealing with the right person. Effective state action, especially in the digital realm, thus depends on enabling reliable and secure identity verification.

Who Am I Talking To? Identity in Public Discourse

To ensure trust in public discourse, it is also important to be able to identify one's digital counterpart. This involves, on the one hand, the question of whether I am communicating with a real person or a machine in a specific interaction. On the other hand, it is not insignificant that people often impersonate others – whether with malicious intent or not. The verification of authentic personal accounts, for example on social media, is thus crucial, regardless of whether real names are used or not. Trust in the authenticity of communication and the reliability of public discourse is therefore directly linked to identification.

Self-Determined Identifiability

Political participation, or the ability to express oneself politically without fear of negative consequences, depends on the success of establishing systems that allow for self-determined management of one's own identity. These systems, whether state-initiated or decentralised, should ideally enable citizens to decide for themselves when they are clearly identifiable, when they are only known by a pseudonym, and in which cases they can also be completely anonymous. Individuals should not be subjected to the pressure of being permanently identifiable and addressable.

Protection Through Anonymity and Pseudonymity

This is where the downside of strong identification systems lies: they can undermine the protection that anonymity and pseudonymity provide. Particularly minorities and marginalised groups often rely on protected contexts to find their own position and voice or to formulate collective concerns. Precisely because digital identities abstract from many physical or social characteristics, they could potentially offer greater equality in terms of services or participation—however, this must be actively facilitated.

The Authoritarian Danger of Permanent Surveillance

Permanent surveillance capabilities and continuously assignable behavioural profiles limit individual autonomy. It is no coincidence that strong identity regimes are often a feature of very asymmetric, often anti-democratic and illiberal contexts, and are used in authoritarian states or border and migration regimes. The growing prevalence of private-sector identity management systems can also be problematic: Here, the potential for unequal treatment poses both security risks and undermines the private autonomy of citizens. This tendency would further intensify if virtual worlds were to become more widely available. In these spaces, much more comprehensive tracking of behaviour and biometric information is possible.

In Conclusion

As long as we communicate digitally, digital identity will remain a structural issue and will bring with it a constant problem of identification and verification. We see that people are communicating less and less in anonymous contexts; this leads to the possibility that a person‘s identity can be determined at any time, even retrospectively, and is increasingly linked to behavioural data. With regard to democracy, these effects are ambivalent. What is needed are identity management systems that allow citizens to decide for themselves how and to what extent they share data and make themselves identifiable.

Further Reading

- Anke, Jürgen / Richter, Daniel 2023: Digitale Identitäten: Status Quo und Perspektiven, in: HMD Praxis der Wirtschaftsinformatik 60: 2, 261 – 282. // *A German-langauge overview article introducing various digital identity concepts, particularly categorising and differentiating possible systems from an informatics perspective*

- Cheney-Lippold, John 2011: A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control, in: Theory, Culture & Society 28: 6, 164 – 181. // *Open-access article that early on shaped the discussion around changing identity and identification procedures. In 2017, the book We Are Data by the same author was published, updating and deepening these arguments.*

- Renieris, Elizabeth M. 2021: Identity in a "Phygital" World: Why the Shift to Machine-Readable Humans Demands Better Digital ID Governance, Centre for International Governance Innovation. // *Opinion piece that particularly addresses the merging of digital and analogue identity practices, arguing for the need for better identity management systems.*

- Thiel, Thorsten 2017: Anonymität und Demokratie, in: Forschungsjournal Soziale Bewegungen 30: 2, 152 – 161. // *A German-language overview article discussing the concept of anonymity, its development in digital contexts, and the relationship between anonymity/identity and democracy.*

Publishing credits & legal notice

Bertelsmann Stiftung
Carl-Bertelsmann Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Responsible for the publication
Kai Unzicker
Senior Project Manager
Telefon +49 5241 81-81405

kai.unzicker@bertelsmann-stiftung.de
www.bertelsmann-stiftung.de
www.upgradedemocracy.de

Authors
Prof. Dr. Thorsten Thiel, Dr. Susanne Kailitz

Design
nach morgen

Picture Credits
Montage Cover: © dehweh - stock.adobe.com

Citation note
Thiel, T. and Kailitz, S. (2024) *Digital Identity and Civil Rights. Visions: Democracy and Technology / Part 3*. Bertelsmann Stiftung. Gütersloh.