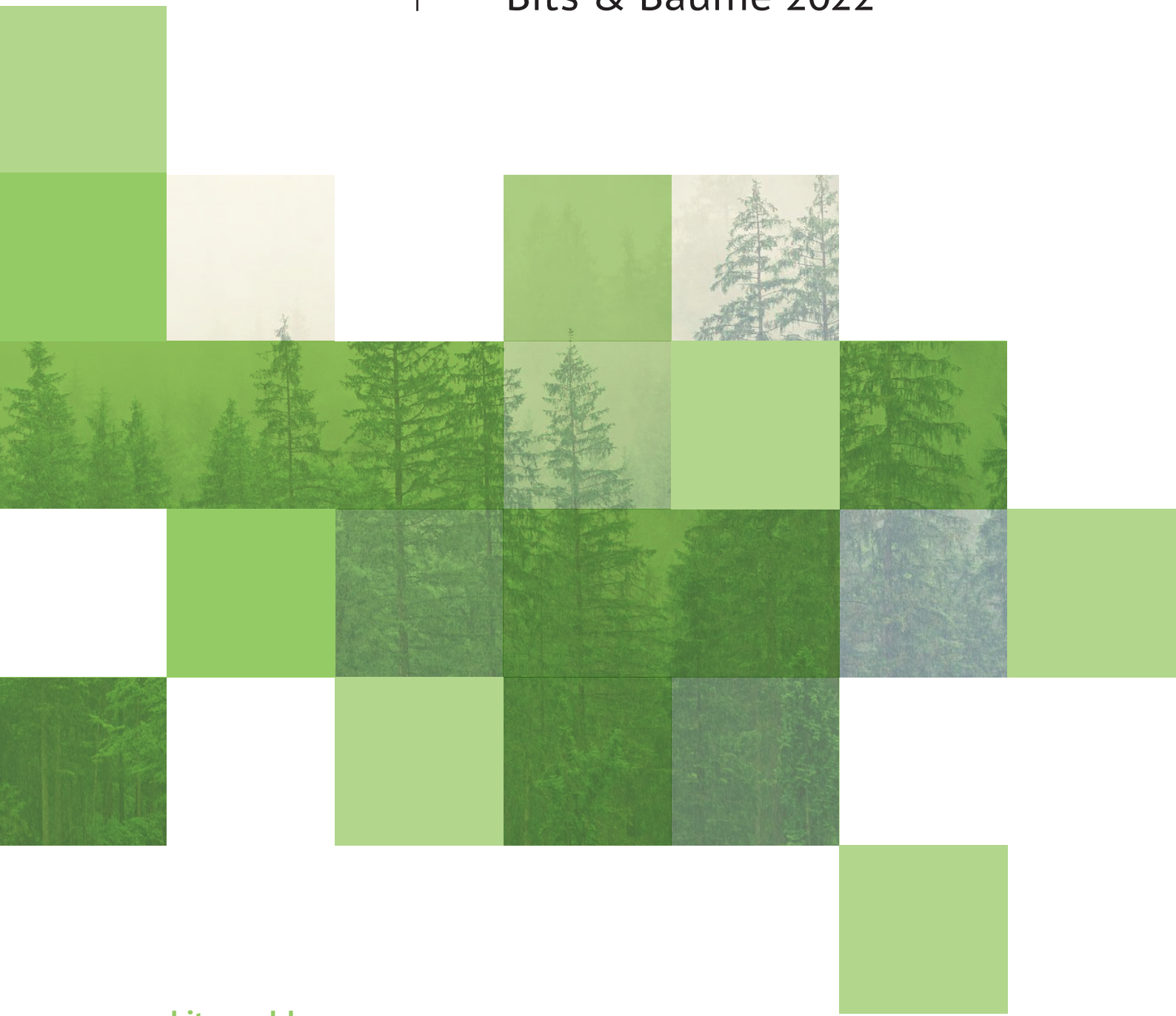
Bits & Bäume

Making digitalisation sustainable and fit for the future

Political Demands
Bits & Bäume 2022



bits-und-baeume.org

PREAMBLE

Thirteen organisations from the fields of environmental protection, digital policy, development policy and science are organising the second “Bits & Bäume” (Bits and Trees) conference for digitalisation and sustainability together with a committed community. We are convinced that political changes are necessary to ensure that digitalisation can contribute better to the urgent social and ecological transformation. We are united by an inclusive understanding of sustainability and the determination to shape a future in which digital transformation plays a positive role and supports and protects people, livelihoods and the environment.

Together, we call on the German government, the European Union and political actors worldwide to swiftly implement our demands. We are aware that these demands do not cover all the policy changes needed to shape a transformative and sustainable digitalisation, so further measures must be developed together with civil society expertise.

sponsored by:

Gefördert durch: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz aufgrund eines Beschlusses des Deutschen Bundestages

gefördert durch DBU Deutsche Bundesstiftung Umwelt

STIFTUNG MERCATOR

Bits & Bäume

Short Version

Making digitalisation sustainable and fit for the future

Political Demands
Bits & Bäume 2022

1 Digitalisation within planetary boundaries

Click on the headline to get to the extended version.

We demand that technological developments are aligned with the standards of nature, climate and resource protection and the preservation of biodiversity. Digital infrastructures and electronic devices must be constructed and operated in a climate-neutral manner, without climate compensation. In detail, this means:

1.1. Digitalisation must be ecologically oriented in order to contribute to fundamental socio-ecological transformations, especially in the energy, mobility, agriculture, industry and consumption sectors. To this end, standards and transparency must be promoted.

1.2 The growth of data flows must be reduced.

1.3. Hardware and digital infrastructure must be durable. For this purpose, a legally guaranteed device neutrality, the right to repair and ownership, and the obligation to publish drivers, tools and interfaces under a Free Software/Open Source license should be encouraged.

2 Global justice and regional empowerment

We advocate a digital transformation that supports a globally just and sustainable economic system. Trade agreements on digital goods and services should not restrict national regulations required to build an independent digital economy locally.

2.1. Local communities, civil society and indigenous peoples must be involved in shaping the global digital economy and related policies.

2.2. In addition to a decrease in the consumption of raw materials for digitalisation in the Global North, we call for responsibility in trading practices with the Global South and a just digital economic governance framework.

2.3. Digitalisation in the agricultural sector must serve global food sovereignty and address environmental goals and the needs of small-scale farmers. Small-scale farmers must be able to operate independently of platforms or seed and agricultural machinery corporations.

3 Redistribution of technological power, democracy and participation

We demand the creation of governance frameworks that control digital monopolies and democratise the digital world. Specifically, we demand that:

3.1. Business models and government actions based on detailed tracking/profiling or otherwise complex behavioural analysis should be prohibited. This ban should include microtargeting, psychometric analyses, geo-, mouse- and eye-tracking. These practices give rise to information and data power that is incompatible with principles of democracy and sustainability. Business models that serve the common good and protect the climate and the environment do not need these practices.

3.2. Opportunities for democratic governance, participation and public-interest-oriented business models are supported.

3.3. Public data must be considered common goods. Publicly financed digital goods and software must be published under a Free Software / Open Source license. Transparency and auditing of data and algorithms must be guaranteed.

4 Justice in digitalisation, sustainable technology design and social issues

We demand that social and ecological justice and the orientation toward long-term peace are fundamental goals of digital transformation. In this context, technology design, education and work must be aligned with strengthening social cohesion. In detail, this means:

4.1. Digital technologies and their use must always be geared towards supporting long-term peace efforts in our society and globally. It is essential that prohibitions and bans in this context are regulated in an international convention. This convention would also ensure that no state that has renounced the use of so-called digital weapons can be threatened with them by other states. Every war is preceded by many wrong political decisions; peace is a long-term project.

4.2. Digitalisation must bring social improvement and should not lead to a deterioration of social and occupational health and safety standards.

4.3. Technology has to be designed according to intersectional-feminist principles and must not perpetuate structural disadvantages and discrimination in society.

4.4. "Universal" access to digitalisation, digital literacy and creative freedom must be supported.

4.5. Users in the digital sector must be consistently protected.

5 Protection of digital infrastructure and IT security

A sustainable democracy needs reliable, secure and trustworthy infrastructures. We, therefore, demand that digital infrastructures are adequately protected and maintained. To realise this, public security must be understood in such a way that IT security and data protection are oriented toward fundamental rights and viable and liveable societies.

5.1. Free and sophisticated eGovernment is a prerequisite for an inclusive and sustainable digital society. Rolling out a free and open nationwide system for secure signatures and authentication is essential in creating a trustworthy and reliable digital information and communication infrastructure for government interactions. All relevant infrastructures must be adequately maintained and kept updated.

5.2. A global digital society – from the use of electronic industrial controls to social communication in digital space – necessitates the confidentiality and integrity of all systems. This necessity requires a consistent defensive orientation of domestic and foreign policy on all digital affairs.

5.3. A minimum standard for IT security and longevity in using digital products must be ensured.

5.4. The vulnerability of the entire digital infrastructure through technical failures, cyber-attacks, etc. should be taken into account when designing infrastructure digitalisation (e.g., energy transition).

Extended Version

Making digitalisation sustainable and fit for the future

Political Demands
Bits & Bäume 2022

1 Digitalisation within planetary boundaries

We demand that technological developments are aligned with the standards of nature, climate and resource protection and the preservation of biodiversity. Digital infrastructures and electronic devices must be constructed and operated in a climate-neutral manner, without climate compensation. In detail, this means:

1.1. Digitalisation must be ecologically oriented in order to contribute to fundamental socio-ecological transformations, especially in the energy, mobility, agriculture, industry and consumption sectors. To this end, standards and transparency must be promoted.

1.1.1. The digital transformation of industry must be aligned with explicit circular economy goals. It must be ensured that companies fulfil their due diligence obligations along the entire value chain. We demand that the envisaged digital product pass covers transparency on greenhouse gas emissions, raw material composition, source of materials and repair and recycling requirements along the entire value chain. A strong EU supply chain law must also cover the deeper supply chain level and the raw materials relevant to digitalisation.

1.1.2. Technologies must be regulated dynamically. Regulations should exceed common efficiency-focused standards and include a transparency obligation for appropriate environmental metrics (e.g., power usage effectiveness, water usage effectiveness, carbon usage effectiveness) as well as social indicators.

1.1.3. Design principles and environmental standards must be developed and implemented. These must be aligned with the circular economy goals. Especially resource-intensive information technologies such as data centres must be obligated to operate in a climate-neutral manner and utilise waste heat.

1.1.4. Server operators must be obligated to publish a CO_2 footprint per service unit (e.g., hour/year). These publications should form the basis of an emissions-reducing governance framework.

1.1.5. Clear standards and responsibilities must be defined for platforms and providers of digital services, especially in the sectors mobility, energy, agriculture and housing, as well as for online consumption. These standards and responsibilities will ensure that the application of the sectors' technologies and

the third-party use of their services contribute to a sustainability-oriented transformation of the sectors. For example, the business activities of mobility platforms should be linked to the condition that their services systematically support users in transitioning to environmentally friendly, climate-neutral mobility.

1.1.6. Environmentally harmful business practices of online retailers, such as the destruction of returned goods, must be prohibited. Additionally, platforms should be required to display rental and repair options more prominently than new purchase options.

1.2 The growth of data flows must be reduced.

1.2.1. We call on the German government and the EU to ban autoplay and similar functions or, as a first step, to at least mandate that they are turned off by default. This call includes, for example, the automated playing of (advertising) videos when visiting websites and looping videos in music apps.

1.2.2. Multiple mobile coverage of the same regions increases electricity consumption and must be avoided. Therefore, national roaming with standardised and fair tariffs must be introduced.

1.3. Hardware and digital infrastructure must be durable. For this purpose, a legally guaranteed device neutrality, the right to repair and ownership, and the obligation to publish drivers, tools and interfaces under a Free Software / Open Source license should be encouraged.

1.3.1. The universal right to install and develop any operating system and software on any device should be enforced. No legal, technical or other obstacles to the general reuse of these devices must be allowed.

1.3.2. To enable the right to repair, the right to ownership and downstream markets around hardware, manufacturers must commit to device neutrality. This device neutrality requires that source codes for drivers, tools and interfaces are published under a Free Software/Open Source license.

1.3.3. Hardware must be subject to mandatory recycling.

1.3.4. Specifications for data standards and interoperability must be developed so that services can be provided by third parties on a cross-hardware and vendor-independent basis. Online services and devices must ensure true interoperability using open standards for all basic functions.

2 Global justice and regional empowerment

We advocate a digital transformation that supports a globally just and sustainable economic system. Trade agreements on digital goods and services should not restrict national regulations required to build an independent digital economy locally.

2.1. Local communities, civil society and indigenous peoples must be involved in shaping the global digital economy and related policies.

2.2. In addition to a decrease in the consumption of raw materials for digitalisation in the Global North, we call for responsibility in trading practices with the Global South and a just digital economic governance framework.

2.2.1. Political actors must take global responsibility for the trade and consumption of raw materials for hardware production. Those raw materials are often mined in conflict regions under inhumane conditions, and their extraction inflicts massive damage to natural ecosystems. Companies must be obligated to respect human rights throughout their entire supply chain and during disposal. Production chains should aim for closed cycles and a reduced usage of raw materials.

2.2.2. In the long term, resource preservation requires an absolute reduction in consumption, with strict resource protection targets.

2.2.3. The digital divide between countries of the Global South and North must be minimised by prioritising knowledge and technology transfer within international development cooperation. In this context, national and regional platforms must be promoted and public data infrastructure and local data processing must be established and expanded, while ensuring data anonymity. These measures are important in ensuring that, in the long term, countries of the Global South are not limited to the role of data suppliers.
For this purpose, cross-border, regional digital markets must be enabled. Countries of the Global South must be allowed to take protective measures and impose customs duties in order to pursue an economic policy tailored to local needs and to achieve regional self-empowerment.

2.3. Digitalisation in the agricultural sector must serve global food sovereignty and address environmental goals and the needs of small-scale farmers. Small-scale farmers must be able to operate independently of platforms or seed and agricultural machinery corporations.

3 Redistribution of technological power, democracy and participation

We demand the creation of governance frameworks that control digital monopolies and democratise the digital world. Specifically, we demand that

3.1. Business models and government actions based on detailed tracking/profiling or otherwise complex behavioural analysis should be prohibited. This ban should include microtargeting, psychometric analyses, geo-, mouse- and eye-tracking. These practices give rise to information and data power that is incompatible with principles of democracy and sustainability. Business models that serve the common good and protect the climate and the environment do not need these practices.

3.2. Opportunities for democratic governance, participation and public-interest-oriented business models are supported.

3.2.1. Public responsibilities, especially in the area of services of general interest and digital infrastructures, should be accessible to democratic oversight. Participatory and collaborative organisational and business models should be adopted. Cooperative economic practices, such as cooperatives or associations, should be de-bureaucratised and digitalised in a legally secure manner. Existing start-up funding programmes should focus on promoting participatory start-ups.

3.2.2. Civil society actors must be involved in political processes on equal terms. Financial resources for this political engagement must be made available.

3.2.3. Participatory technology assessment with equal involvement of science and civil society experts (in line with 3.2.2) should take place before technologies are developed or used, especially in areas of critical infrastructure and providing public services. This involvement must also be possible on one's own initiative.

3.2.4. Civil society organisations and science must be involved in both developing state-run funding programmes and selecting programme projects (in line with to 3.2.2).

3.2.5. A technology impact assessment should consider, in particular, criteria for the social benefit of an application. These criteria include an orientation towards the common good, compliance with the Universal Declaration of Human Rights, contribution to achieving the Paris Climate Agreement and the Sustainable Development Goals, use of Free Software / Open Source, accessibility, open interfaces between different digital services and platforms, focus on IT security and data protection. We demand the mandatory publication of the analyses including the data protection impact assessments (DPIA) according to Art. 35 of the EU General Data Protection Regulation (GDPR).

3.2.6. Non-commercial platforms as alternatives to only profit-oriented digital corporations must be established to ensure that the common good is adequately catered for. In this context, participatory forms, such as councils with civil society participation, can ensure that the service is not aimed at mere profit-making interests. For media platforms, public service models can be used, however, without creating a state monolith. Technology design must consider principles of informational sustainability (from 3.3.2).

3.3. Public data must be considered common goods. Publicly financed digital goods and software must be published under a Free Software / Open Source license. Transparency and auditing of data and algorithms must be guaranteed.

3.3.1. Public data and information must be subject to public participation and accountability and must be provided free of charge, permanently and openly, wherever feasible. Ensuring this access includes aligning all publicly funded or co-financed tangible and intangible goods, software and services, such as mobility data on multimodal sustainable travel, with the principle of openness by publishing them under Free Software/Open Source licences.

3.3.2. Common and established practices and guidelines for informational sustainability should be widely shared and encouraged in order to ensure the long-term viability of the digital space. This viability includes Free Software/Open Source Software that can be used, examined, distributed and improved for any purpose – as well as open standards, ecological Sustainability by Design and Privacy by Design. These concepts and guidelines must also be established in public procurement, especially in purchasing and contracting (implementation of EU Directives 2014/24/EU, 2014/25/EU, 2014/23/EU) and be applied according to "Public Money Public Code" and/or "Public Money, Public Good".

3.3.3. Competition and antitrust laws must be reformed to combat the formation of digital monopolies and dissolve existing monopolies. For this purpose, organisational and ownership structures must be adapted (in accordance with 3.2.1). Where this process is not possible due to a lack of legislative competence, dependency on monopolies must be eliminated. At a minimum, this process requires established practices and guidelines of informational sustainability (from 3.3.2).

3.3.4. Decisions made by IT systems in publicly relevant infrastructures cannot be a "black box". They must be made available transparently and comprehensibly under Free Software / Open Source licences. This availability also applies to work and business processes outside public institutions if they affect the health and management of employees.

3.3.5. The protection of participation and fundamental rights in automated decision-making systems must be guaranteed by making the basis for decisions (data and algorithms) available for independent review. The review boards should be supervised by civil society and should be able to formulate requirements, sanction non-compliance and include an ombudsperson's office that can investigate individual complaints. The following enforcement deficit points concerning the GDPR must finally be resolved: the consistent prevention of detailed profiling/tracking, the adoption (or termination) of appropriate transatlantic data protection rules or the enforcement of fairness principles according to Art. 5 GDPR.

4 Justice in digitalisation, sustainable technology design and social issues

We demand that social and ecological justice and the orientation toward long-term peace are fundamental goals of digital transformation. In this context, technology design, education and work must be aligned with strengthening social cohesion. In detail, this means:

4.1. Digital technologies and their use must always be geared towards supporting long-term peace efforts in our society and globally. It is essential that prohibitions and bans in this context are regulated in an international convention. This convention would also ensure that no state that has renounced the use of so-called digital weapons can be threatened with them by other states. Every war is preceded by many wrong political decisions; peace is a long-term project..

4.1.1. This international convention should regulate a ban on the export and use of so-called digital weapons and armed drones and their digital infrastructures..

4.1.2. We want international cooperation that contributes to civil peacekeeping and enables the long-term pacification of conflicts and reconstruction and promotes sustainable development that allows all people to participate fully, effectively and equally in society. Instead of strengthening military capabilities, we call for a permanent increase in public spending for peace-oriented development cooperation at an equal level and a foreign policy oriented towards global peace and common security.

4.2. Digitalisation must bring social improvement and should not lead to a deterioration of social and occupational health and safety standards.

4.2.1. Platforms and tech companies should be regulated to ensure that new forms of work, especially in the area of click- and crowd-working, do not endanger workers (Good Work by Design) and that workers' rights of access to their representatives are realised. In addition, fair payment for creative and media sectors and the promotion of alternative payment models should be implemented, e.g., digital anonymous micropayment oriented towards design and environmental standards (mentioned in 1.1.2 and 1.1.3).

4.2.2. The federal government should finance a smart meter rollout for all electricity, i.e., self-generated or drawn from the grid, for people with low electricity consumption (often tenants). For people with high electricity consumption (often single-family homeowners), a smart meter installation is usually financially worthwhile because they have sufficient flexibility options or efficiency incentives to (over compensate for the costs of a smart meter. These people with high electricity consumption should therefore finance the mandatory installation and operation of smart meters themselves.

4.3. Technology has to be designed according to intersectional-feminist principles and must not perpetuate structural disadvantages and discrimination in society.

4.3.1. Digital technologies are not neutral. They are created by people and can (re-)produce social inequalities. The design of digital technologies must therefore always take into account intersectional-feminist principles in order to foster the necessary social change. Such principles include making visible and paying attention to care-work issues and disadvantaged and marginalised groups, as well as to issues of intersectional justice and inequality. The objective of any technology must be to actively counteract any existing discriminatory structures, including discrimination based on age,

gender, sexual orientation or identity, marital status, (relative) poverty, education, health/disability, origin, skin colour, language or religion.

4.3.2. Communication platforms must actively prevent hatred and violence against marginalised groups. This prevention must be regulated in a legally binding manner.

4.3.3. Technologies should not be developed and designed by a homogeneous group of people but by diverse teams. Care and solidarity should be at the heart of development - not exploitation and egoism. Marginalised and disadvantaged groups, especially women, queer people and people affected by racism and ableism, should have an adequate voice and be heard in the digital sphere. These groups must be actively empowered to participate in the design of technology; otherwise, the discriminatory structures of society will be perpetuated.

4.4. "Universal" access to digitalisation, digital literacy and creative freedom must be supported.

4.4.1. All people must be given the opportunity to participate in digitalisation. This participation requires government funding programmes that invest in digital literacy and open technology education, such as open workshops, and, in particular, include actors who have been excluded from funding to date, such as those involved in digital volunteering.

4.4.2. Curricula and advanced training must aim to enhance digital literacy instead of teaching a specific software application.

4.4.3. To be able to participate in technological development, people of all ages must be given "universal" and equitable access to digitalisation and (technology) education in the spirit of lifelong learning. Apart from promoting digital literacy, this education must include sociological, ethical and ecological components that enable a reflection on the social impact of technologies. Learning must thus be understood as cross-institutional and cross-disciplinary, and the education system must provide the necessary creative freedom.

4.5. Users in the digital sector must be consistently protected.

4.5.1. Patent/copyright law and practice should be realigned towards a fair and free digital knowledge order. Commercial exploiters must no longer be unilaterally favoured at the expense of the authors. Instead, fair compensation models must be created between users and creators. Content for education and teaching must be easy and risk-free to use and the persecution of non-commercial use must be ended. A new copyright law must explicitly allow and promote free works such as software and media, copy-left licenses and a digital commons. Patenting of software or living beings such as plant or animal DNA must be prevented or ended. In particular, indigenous peoples affected by this patenting must be supported everywhere and immediately.

4.5.2. In data protection law, the "protection of personal data" is to be replaced by the "protection of people in data processing operations". Ensuring this change also includes the processing of anonymous data if the result has an impact on individuals, groups of people or society. Data retention must be abolished.

4.5.3. We demand the right to anonymity. Authenticity on the Internet must not be at the expense of anonymity and must not be bought through identification procedures. Those who use anonymous

communication options, such as Tor or VPN, must not be subjected to further persecution and reprisals. It must be clarified by law that operators may not be prosecuted for statements made by third parties via their services. Related to this, there must be export bans on any IT systems that can be used for surveillance, censorship or persecution.

5 Protection of digital infrastructure and IT security

A sustainable democracy needs reliable, secure and trustworthy infrastructures. We, therefore, demand that digital infrastructures are adequately protected and maintained. To realise this, public security must be understood in such a way that IT security and data protection are oriented toward fundamental rights and viable and liveable societies.

5.1. Free and sophisticated eGovernment is a prerequisite for an inclusive and sustainable digital society. Rolling out a free and open nationwide system for secure signatures and authentication is essential in creating a trustworthy and reliable digital information and communication infrastructure for government interactions. All relevant infrastructures must be adequately maintained and kept updated.

5.2. A global digital society - from the use of electronic industrial controls to social communication in digital space - necessitates the confidentiality and integrity of all systems. This necessity requires a consistent defensive orientation of domestic and foreign policy on all digital affairs.

5.2.1. IT security vulnerabilities must no longer be exploited by (security) authorities, whether directly via homebrew (e.g., "BKA-Trojaner"), via contract work (e.g., "Digitask-Trojaner") or by hiring such services (e.g., "Pegasus"). All German authorities are to be legally obliged to report discovered IT security vulnerabilities to manufacturers via responsible disclosure and to publish them. Furthermore, Section 202c of the German Criminal Code (StGB), the so-called "HackerParagraph", should be abolished, thus decriminalizing IT security research. Germany must work within the EU, transatlantically and globally to ensure that government agencies commit to closing IT security gaps. This closure includes moving away from crypto bans or the strategic weakening of cryptographic systems.

5.2.2. "Offensive means of action" in the military sphere - for example, through hackbacks or by government agencies infiltrating foreign systems in digital space - must be consistently banned. Germany must work within the EU, transatlantically and globally to ban so-called digital weapons.

5.3. A minimum standard for IT security and longevity in using digital products must be ensured.

5.3.1. In the case of proprietary software, the "polluter pays" principle should be introduced for IT security vulnerabilities. This principle implies that providers, operators and manufacturers are liable for omissions and damages and that, therefore, an insurance obligation should exist. There should also be an operating and update guarantee for a typical product service life for all software components in devices, for software and for any necessary backends. In the commercial operation of digital services, providers must be responsible for the IT security of the service, including, for example, due diligence regarding the installation of security updates.

5.3.2. The most recent development tools for improving IT security, maintainability and long-term usability of software should always be made publicly available.

5.4. The vulnerability of the entire digital infrastructure through technical failures, cyber-attacks, etc. should be taken into account when designing infrastructure digitalisation (e.g., energy transition).

5.4.1. Digital infrastructure and devices can be made resilient through various measures. In addition to observing the classic IT security principles, this resilience also necessarily includes the possibility of short-term offline operation, e.g., via the islanding capability of smaller cells or non-digital operating processes for emergencies.

5.4.2. Training and payment of the necessary technical personnel must be sufficient and secured for the long term.

See online version