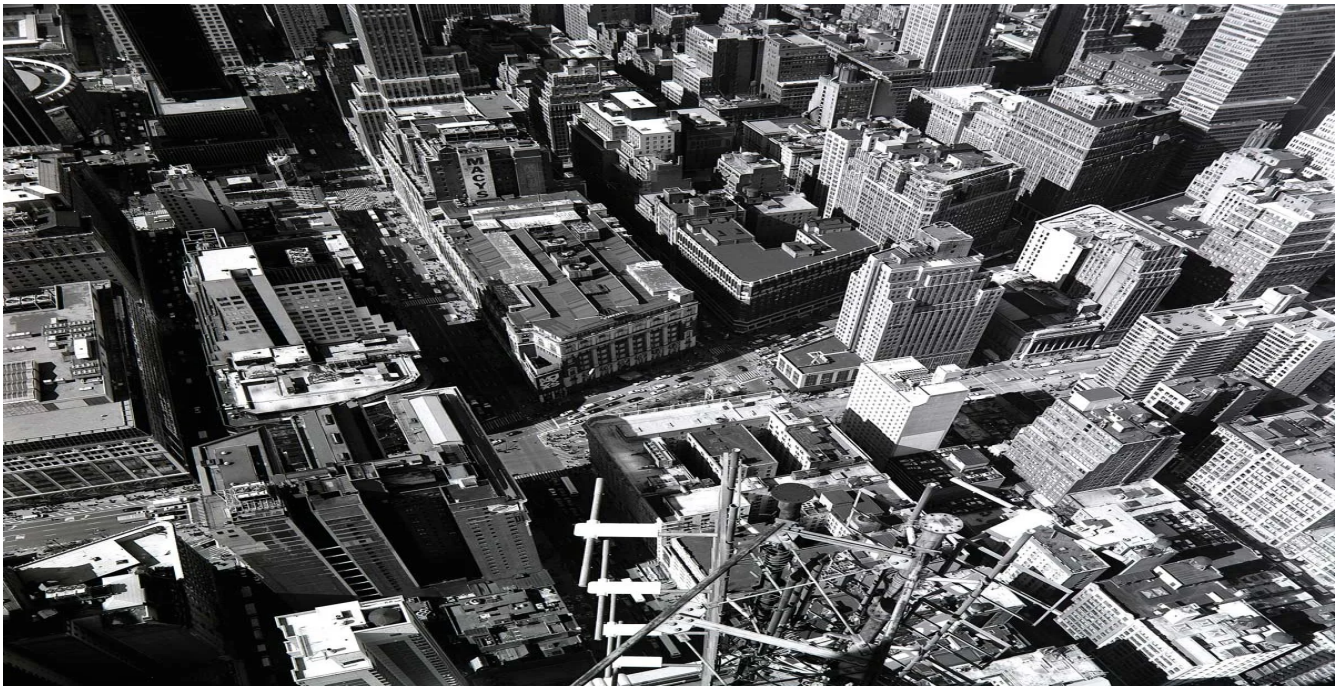
Data and Artificial Intelligence



Arne Maasik. NYC Shots 4314. Sublimation print on polyester fabric. 2005 (fragment of the work)

Living in a digital and data-driven society means that, in exercising public authority, the state collects data about people’s health, education, family, property, livelihood and other aspects of their lives. As Estonia began building its digital state almost 30 years ago, our public authorities hold a considerable amount of data and have extensive experience in using it.

The mere existence of data does not necessarily mean that the data are of good quality — accurate and complete — or that they are used wisely, consciously and lawfully. Only as much data should be collected as is permitted by law and necessary. Collecting data ‘just in case’ does not guarantee better public services or faster solutions. Not every problem in society is caused by a lack of data.

As a general rule, the creation of large centralised data repositories should be avoided. Before bringing together different types of personal data, we should ask why certain data are kept separate and why there are strict limits on who may access which data; what values and whose fundamental rights are protected by keeping the data separate. Why does the

Constitution sometimes prescribe what may seem an excessively slow and cumbersome route to accessing data — for example, requiring judicial authorisation for an investigative measure or requiring requests to be made to other authorities in order to access data? The answer lies in the protection of fundamental rights: collecting and using data may restrict a person's fundamental rights. A balance must therefore constantly be sought between the benefits of a data-driven society and the protection of fundamental rights.

The development of artificial intelligence brings a new dimension to the search for that balance. The use of AI may involve, for example, a chatbot on a public authority's website, an AI-based tool for analysing data and identifying patterns, or an official using an automated system's recommendation or transcription tool to support decision-making. Krista Fischer, Professor of Mathematical Statistics at the University of Tartu and a member of the Estonian Academy of Sciences, has explained that artificial intelligence is not magic: it is based on well-known mathematical methods. What is new is the enormous computing power now at our disposal, enabling vast quantities of data to be analysed extremely quickly.

Because of the intensity, speed and scale at which artificial intelligence operates, questions concerning AI are not merely technical. This is not simply a technology, but a technology with potentially far-reaching implications for fundamental rights and constitutional principles — for example, for the nature of our public space and for how much automated data collection the Constitution permits.

We should take a constructively critical approach to AI-based tools and ask whether they are of sufficiently high quality to be used in areas such as social services, healthcare or education, where errors caused by technology can come at a high price. Not everything that is technically possible is necessarily needed or compatible with the protection of fundamental rights. From the perspective of fundamental rights, we must also ask who gains access to the personal data we enter into an AI-based system in Estonia — and in which countries the servers and systems receiving those data are located.

People must always know when the state is using artificial intelligence in its interactions with them or in making a decision about them. This ensures transparency and helps maintain trust. Public administration must not become a 'black box': even when artificial intelligence is used, the principles of administrative procedure must be observed.

Critical discussion about the use of artificial intelligence must therefore also take place within Estonia’s constitutional institutions.

Publication of Orthophotos

Several people contacted the Chancellor with concerns that the Estonian Land and Spatial Development Board publishes high-resolution orthophotos (top-down aerial images) and oblique aerial photographs (images taken at an angle) on the Estonian Geoportal, showing people’s homes, gardens and belongings in considerable detail.

Orthophotos and oblique aerial photographs are necessary for the performance of state functions. They are needed, for example, to update topographic maps, for spatial planning, and for rescue and national defence purposes. Achieving these objectives, however, does not require making publicly available photographs that show in detail someone’s pram, washing hanging on the line, sports equipment and other belongings.

No one is required to share their private life with the public or to tolerate curiosity-driven scrutiny of parts of their property that cannot be seen from the street. The right to the inviolability of private life may be restricted only on the grounds set out in § 26 of the Constitution and based on a law that is in conformity with the Constitution.

The Chancellor found that a distinction must be made between taking aerial photographs and making them available to the public without restriction. The state should not stop collecting high-quality spatial data, but its practice of making those data publicly available should be reviewed. Orthophotos and oblique aerial photographs should therefore be made available in a way that takes better account of people’s fundamental rights. Possible measures could include publishing photographs after a time delay, applying general blurring to the images, or allowing access to the most detailed photographs only after the user has authenticated themselves.

After receiving the Chancellor’s opinion, the Estonian Land and Spatial Development Board changed its practice. The aerial photographs taken in 2025 were processed into orthophotos with limited resolution, taking account of both the right to the inviolability of private life and national security needs.

The Ministry of Economic Affairs and Communications has circulated to stakeholders a legislative proposal to amend the Spatial Data Act and other Acts. Among other things, the proposal considers reducing the resolution of orthophotos and oblique aerial photographs available to the public, publishing the data after a time delay, and making high-resolution photographs available only to authenticated users with a legitimate interest.

Estimating Wildlife Population Density Using Artificial Intelligence

The Estonian Environment Agency uses species-identification technology based on the random encounter model (REM) in wildlife monitoring. This methodology has been used to process camera-trap recordings since 2024. Camera traps may also capture images of people, although recording human activity is not the purpose of placing the cameras in the wild or processing the images they capture.

The Chancellor analysed whether the use of an AI-based solution in wildlife monitoring complies with the requirements for the protection of fundamental rights. The Chancellor's advisers met with the Estonian Environment Agency team responsible for developing and implementing the species-identification technology, took part in installing camera traps in monitoring areas, and observed how the recorded data were processed using the species-identification technology.

As long as camera traps continue to be used as they are now — for limited periods and in places that are rarely visited, with people appearing in the images only rarely and by chance — the actual risk to people's rights remains largely theoretical. The same applies to the AI-based analysis of the recordings. The purpose is to use camera-trap recordings to identify animal species and estimate their numbers. Artificial intelligence is not used to search the recordings for people.

The Chancellor considered it important that any restriction of people's fundamental rights resulting from the use of new technology should be proportionate. This means that the Estonian Environment Agency must place camera traps in places that are rarely visited, schedule monitoring periods mainly for early spring and late autumn, and inform people that cameras are being used. It is also important that the species-identification software is configured to identify animal species, not people who happen to enter the cameras' field of

view.

If a photograph taken by a camera trap showing a person needs to be forwarded to a supervisory authority or law enforcement authority for the purposes of proceedings, the Estonian Environment Agency must delete the photograph after forwarding it. No legislation permits such a photograph to be retained in the Agency's database. If camera traps are to be used for other purposes in the future — for example, to identify and penalise people who dump waste in forests or poachers — the Riigikogu must authorise this by law.

Requesting Bank Account Statements

In 2025, the Chancellor drew attention to the fact that several authorities had access to bank account statements through the Enforcement Register even though the register had no statute and there were no clear legal grounds for requesting bank account statements in administrative proceedings.

The Chancellor also submitted an opinion on the Bill prepared to resolve the problem.

The Chancellor considered it appropriate that the Bill sought to establish clearly by law the authorities' access, through the Enforcement Register, to information subject to banking secrecy, including bank account statements. This means that the law must specify what data a particular authority may use in carrying out its duties and what mechanisms are available for overseeing such use. As this constitutes a very serious restriction of fundamental rights (§§ 19 and 26 of the Constitution), granting such access must be a thoroughly considered and carefully defined exception.

It is important that, in addition to resolving individual issues, the provisions of § 88 of the Credit Institutions Act governing banking secrecy should also be reviewed in the near future. It is necessary to assess whether all the authorities listed in that section actually need access to information subject to banking secrecy for the performance of their duties and, where such access is necessary, in what circumstances and to what extent it should be granted.

When regulating access to information subject to banking secrecy, it must be borne in mind that a bank account statement, for example, contains so much information about a person and their circle of contacts that it can be used both to profile and, in a certain sense, to track them. Allowing access to an account statement is therefore comparable to requesting communications data or, in some cases, even to conducting a surveillance activity. In criminal

proceedings, communications data may be requested and surveillance activities conducted only where certain criminal offences are suspected and on the basis of judicial authorisation, or in certain cases authorisation from the Prosecutor’s Office. Moreover, requests for communications data reveal only the fact that a call took place or location data, not the content of messages.

For these reasons, particularly careful consideration must be given to whether, and in what circumstances and subject to what conditions, access to bank account information may be permitted in administrative proceedings. When adopting such legal provisions, it must also be ensured that people’s fundamental rights are protected. In other words, access to information subject to banking secrecy must be regulated with the same care and attention as surveillance activities.

Access to bank account statements must be exceptional and limited. The state must therefore lay down in law rules on whether an authority may store such information subject to banking secrecy, including an account statement, in its own database; how long the information may be retained there; whether and for what purposes it may be used further, for example by linking it to another database or sub-register; and whether and when the person whose banking information has been accessed by a state authority must be informed that the information was requested.

Data of a Deceased Gene Donor

The Chancellor was contacted with a concern that the Estonian Biobank does not disclose whether a person was a gene donor or release the person’s genetic data after their death.

The Chancellor found that the requirements laid down in the Human Genetic Research Act are not contrary to the Constitution. Gene donation is based on trust. If, during their lifetime, a gene donor made an explicit declaration of intention allowing their data to be used in the interests of their children’s health, the law does not prevent this. If no such declaration of intention was made, information about a deceased gene donor cannot be obtained from the Estonian Biobank.

Data Collected About Minors

The possible use of artificial intelligence is now also being discussed in child protection work. At this stage, AI is seen as one possible tool for helping to prevent serious crimes committed by minors.

The Child Protection Act already sets out a list of data that a child protection official may use in carrying out their duties. The list is extensive and includes information about a child's health, offences, failure to fulfil the obligation to learn, and other matters. The Act also allows a child protection official, for the purpose of assessing a child's need for assistance or providing assistance to the child, to process the personal data of the child's parent, a person raising the child, a family member of the child, and a person belonging to the child's social network.

A child protection official may also share this information with other specialists, including the police, where their involvement is necessary to assess the child's need for assistance or to provide assistance. Information may, however, be shared only to the extent necessary for achieving that purpose.

The Child Protection Act requires everyone to report a child in need of assistance. There is therefore a legal basis for ensuring that information needed to assist such a child reaches a child protection official.

If AI could take over some of the technical work currently performed by child protection officials and leave them more time to help children, its use should certainly be considered. At the same time, technical tasks must be clearly distinguished from substantive assessment and decision-making. The former may perhaps be entrusted to a machine; the latter may not.

Nor can the aggregation of information about a child stored in different databases be regarded as a merely technical operation. Before deciding to bring all such data together, careful consideration must be given to what data are collected, from which database, and for what reason. It must also be clear who may access the aggregated data and for what purposes they may be used.

AI must certainly not be used to create a consolidated register of children's education, health and other data and then, on the basis of those data, classify children as problematic or non-problematic. The Constitution requires the state neither to know more about a person's private life nor to interfere in it more than is strictly necessary. A child's data must therefore

not be disclosed to anyone unless it is clear that doing so genuinely helps the child, that the objective cannot be achieved in another way, and that the benefits outweigh the harm.