



2/2022

#### **Redakcja Kwartalnika Naukowego Prawo Mediów Elektronicznych**

**Redaktor naczelny:** prof. dr hab. *Jacek Gołaczyński*, UWr

**Sekretarz Redakcji:** dr *Aleksandra Klich*, USz

**Członek Redakcji:** dr *Krzysztof Garstka*, Uniwersytet w Cambridge

#### **Członkowie rady programowej:**

**Przewodniczący:** dr hab. *Wojciech Wiewiórowski* (UG, Europejski Inspektor Ochrony Danych)

#### **Członkowie:**

r.pr. *Włodzimierz Chróścik*

adw. *Rafał Dębowski*

dr hab. *Sviatlana Fursa*, prof. nauk prawnych Kijowskiego Narodowego Uniwersytetu im. Tarasa Szewczenki

dr hab. prof. *Marlena Jankowska*, prof. nadzw. UŚ

adw. *Xawery Konarski*

prof. Avv. *Michele Angelo Lupoi*, Uniwersytet Boloński

prof. dr hab. *Jacek Mazurkiewicz*, UZ

prof. dr hab. *Radim Polcak*, Uniwersytet w Brnie

dr hab. *Grzegorz Sibiga*, INP PAN

dr hab. *Piotr Stec*, prof. nadzw. UO

dr hab. *Dariusz Szostek*, prof. nadzw. UO

prof. dr hab. *Grażyna Szpor*, UKSW

prof. dr hab. *Andreas Wiebe*, Uniwersytet w Getyndze

#### **Recenzenci:**

dr hab. *Andrzej Adamski*, prof. nadzw. UMK

prof. *Zsolt Balogh*, Uniwersytet Corvinus Budapeszt

prof. dr hab. *Sławomir Cieślak*, UŁ

dr hab. *Kinga Flaga-Gieruszyńska*, prof. nadzw. USz

prof. dr hab. *Jacek Górecki*, UŚ

prof. em. dr *Wolfgang Kilian*, University of Hannover

prof. hab. dr *Vytautas Nekrosius*, Uniwersytet Wileński

dr hab. *Marek Świerczyński*, prof. nadzw. UKSW

prof. *Richard Warner* Ph.D, Chicago – Kent College of Law

#### **Adres redakcji:**

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,

Centrum Badań Problemów Prawnych i Ekonomicznych

Komunikacji Elektronicznej

ul. Uniwersytecka 22/26, 51-145 Wrocław

e-mail: [pme@beck.pl](mailto:pme@beck.pl)



C.H.BECK

#### **Wydawca:**

Wydawnictwo C.H. Beck

ul. Bonifraterska 17

00-203 Warszawa

tel.: 22 33 77 600

[www.czasopisma.beck.pl](http://www.czasopisma.beck.pl)

Nakład: 250 egz.

## Spis treści

|                                                                                                                                                                                                                                                 |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| The threat to national security and private data collection of the state in the eyes of Human Rights<br><i>Romane Gielnik</i> .....                                                                                                             | 4  |
| Oprogramowania oparte na sztucznej inteligencji w sądach na całym świecie: praktyka, perspektywy i wyzwania mające znaczenie dla Węgier i Europy Środkowej<br><i>Kinga Kálmán, Laura Olga Kiss, Kitty Mezei, Boldizsár Szentgáli-Tóth</i> ..... | 16 |
| Elektroniczna licytacja nieruchomości<br><i>Krystyna Rogala</i> .....                                                                                                                                                                           | 28 |
| <i>LegalTech</i> w kancelarii komorniczej<br><i>Klaudia Maciejewska</i> .....                                                                                                                                                                   | 37 |

## Contents

|                                                                                                                                                                                                                                      |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| The threat to national security and private data collection of the state in the eyes of Human Rights<br><i>Romane Gielnik</i> .....                                                                                                  | 4  |
| Artificial Intelligence-based software in courts around the world: relevant practice, experience, and challenges for Hungary and Central-Europe<br><i>Kinga Kálmán, Laura Olga Kiss, Kitty Mezei, Boldizsár Szentgáli-Tóth</i> ..... | 16 |
| Online judicial auction of real estate<br><i>Krystyna Rogala</i> .....                                                                                                                                                               | 28 |
| <i>LegalTech</i> in bailiff offices<br><i>Klaudia Maciejewska</i> .....                                                                                                                                                              | 37 |

Szanowni Państwo,

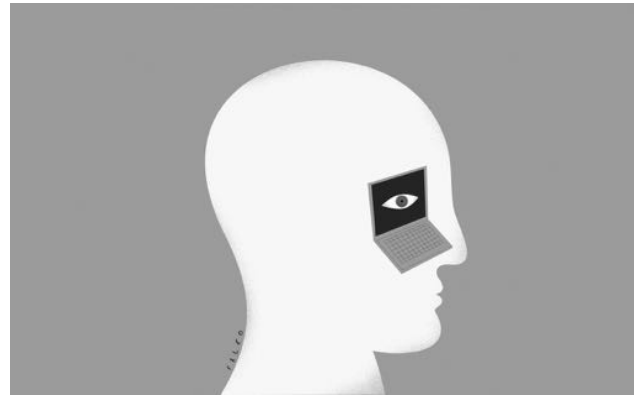
z przyjemnością przedstawiam drugi w 2022 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. W bieżącym numerze kontynuujemy prezentowanie publikacji poświęconych zagadnieniom prawnym, które mają związek z nowoczesnymi rozwiązaniami technologicznymi. O różnorodności tekstów, do zapoznania z którymi pragniemy Państwa zachęcić, świadczy to, że w bieżącym numerze prezentujemy publikacje, w których autorzy omawiają zarówno zagadnienia mające charakter uniwersalny, jak i specjalistyczne, uwzględniające specyfikę wykonywania konkretnych zawodów prawniczych. W numerze znajdziecie Państwo teksty, w tym anglojęzyczny, w których autorzy poruszają zagadnienia związane z zagrożeniami bezpieczeństwa narodowego i prywatnego gromadzenia danych z perspektywy praw człowieka, a także publikację poświęconą oprogramowaniu opartemu na sztucznej inteligencji w sądach na całym świecie z perspektywy stosowania odpowiednich praktyk, doświadczeń i wyzwań krajów Europy Środkowej. Zachęcamy także do zapoznania się z publikacjami uwzględniającymi wykorzystywanie nowoczesnych technologii w praktyce zawodu komornika sądowego. W tym zakresie autorzy omawiają wykorzystanie narzędzi LegalTech w kancelarii komorniczej, a także przybliżają specyfikę prowadzenia elektronicznej licytacji nieruchomości.

Niezmiennie proponujemy współpracę i publikację artykułów, glos czy recenzji wszystkim tym autorom, którzy podejmują tematykę wpływu nowych technologii na prawo prywatne lub publiczne. Zapraszamy do publikacji na łamach Prawa Mediów Elektronicznych, a także do kontaktu z nami pod adresem: [pme@beck.pl](mailto:pme@beck.pl)

Zapraszam Państwa do interesującej lektury  
prof. dr hab. *Jacek Gołaczyński*  
Redaktor naczelny

# The threat to national security and private data collection of the state in the eyes of Human Rights

Romane Gielnik<sup>1</sup>



Drawing by Carlos Alejandro Chang Falco, Cuba.

In this article, it is debated on how the collection of individual's private data by the State affects Human Rights. The peculiar context in which intelligence took its place in our societies has created all its traits and aspects we have today. It has been developed in the age of the Cold War and the War on Terror, a very politically uncertain part of history, which led most governments to fear for their safety. Also, the simultaneous rise of the Digital Age, since the 1950s, nourished this common fright: a new, unknown and unmastered tool was being spread in the hands of all individuals. Two main issues were then confronting each other: the need to preserve the individuals' security as well as their right to privacy and others Human Rights. The interests seemed to oppose each other: to grant a total right to privacy to individuals rhymed with a lack of surveillance of the State on individuals and hence the inability to protect their citizens, when the collection of private state seemed to intrude the right to privacy and so weaken democracy, freedom of opinions and others. If the two notions are opposing, it does not, however, necessarily mean they are contradicting each other: norms should evolve according to the society they serve.

## Introduction

In a recent case of 18 November 2021, at the Court of Justice of the European Union, the Advocate General *Manuel Campos Sanchez-Bordona* formulated the general principles of data collection and retention by the Member States: he held that „the general and indiscriminate retention of traffic and location data relating to electronic communications is permitted only in the event of a serious threat to national security” and added that „national legislation which requires electronic telecommunications undertakings to retain traffic data, on a general and indiscriminate basis in the context of an investigation into insider dealing or market manipulation and abuse, is contrary to EU law”<sup>2</sup>. Such principles have been held before in the European's case law, and are now considered as the basis for further development of legislation on the regard of collection and retention of data relating to electronic communications. However, nowadays, the States collect the data of their own citizens in the name of national security.

If spying is a very old method of getting information, global surveillance arose only around the late 1940s, and developed mainly in the context of the Cold War, and later on the rising of terrorism, with historical events such as the attack on the Twin Towers of the 11 September 2001. One of the first known international agreements on global surveillance is the UKUSA Agreement, which aims for cooperation in signal intelligence between its members, such as the United States, Canada, the United Kingdom and others. Officially enacted in 1946, the existence itself of the treaty was known to the public more than 50 years later, in 2005. A few years later a controversy arose about the treaty and the practice to which it led. The 2013 National Security Agency leaks of the United States of America accused members of the treaty

<sup>1</sup> The author is a student at the University of Lille, France, from the Bachelor of International and European Law, currently a member of the Erasmus+ program in the University of Wrocław, Poland.

<sup>2</sup> Opinion in Joined Cases C-793/19 and C-794/19, in Case C-140/20, and in Joined Cases C-339/20 VD and C-397/20 SR.

to purposefully spy on each other's citizens so as to share information on their citizens.

On the one hand, personal data refers to any information that serves to identify an individual, whether directly or indirectly, such as a full name, scan of the iris of the eye, IP address or card number, such information is known as „identifiers“. On the other hand, private data is the one that is not usually disclosed, in accordance with national legislation, because it is considered to be a part of the intimacy of the individual. Its collection by a State refers to the concept of mass surveillance, the indiscriminate monitoring of a population, mostly via the means of new technologies, such as a phone, surveillance camera footage, or the use of the Internet.

This concept is known for its controversial aspects: the concept itself of mass surveillance implies interference with the individual's right to privacy, and the potential further consequences on the freedoms of individuals, such as expression and protest (for the purpose of this work, the surveillance of known criminals will not be approached. This includes matters such as the collection of data in criminal cases, namely those aiming at legitimate prevention, investigation and detection or prosecution of criminal offences and the execution of adequate penalties). Lastly, national security refers to the prevention of all threats to the territorial integrity, the economic and ecological security, the physical safety of people, as long as there is social and political stability of the State. It can mean the prevention and protection against natural disasters, national defence via armed forces, digital security, health and prevention of criminal interference... or mass surveillance.

Mass surveillance developed in the objective to keep safe all human beings on the State's territory, which is why it gained strength in the Cold War and the early 2000s, as the world faced a rise of terrorist attacks. However, when such surveillance becomes so massive that most common individuals are spied on, it may cause damages to any democratic society. Indeed, the government is then able to restrict as it wishes the freedom of thought and political opinion, which breaches the right to privacy as a fundamental Human Right, via legal norms such as the European Convention on Human Rights in its article 8 „right to respect for private and family life, home and correspondence“.

The complex choice of the use of mass surveillance is inherently tricky, and almost paradoxical. How can one choose between security or freedom? There must be an equilibrium that has to be found between the two notions that guarantees both on legal grounds, while answering to the new challenges of the Digital Age. In other words, the issue raised here must be understood as: „To what extent can a State collect private and personal data in the name of national security, without violating fundamental Human Rights?“

Surveillance rose in a peculiar context. In the last century, the world suffered from many interstate conflicts that grew alongside the development of the Digital Age, causing them both to naturally have a strong connection. However, this development led to paradoxical legal questions that are yet to be answered. This means that new threats arose, to which new means of defence and protection shall be developed as an adequate answer to this evolution. However, every progress opens a new legal field, in which legislation needs to be built: law must adapt to the reality of its contemporary world, which includes the protection of Human Rights in all aspects. In the end, these correlated evolutions answer each other very closely: if one makes a move, the other will too, in the same way of a „question/answer“ game mechanism. There needs to be a balance that guarantees both safety and freedom of the individual, according to the various interests and values of a State, as both notions may be opposites, but not necessarily contrary to each other, which may lead to consider a possible coexistence of both of them.

## The rise of surveillance in a peculiar context

The ways of attacking a State were completely changed during the 20<sup>th</sup> century, which led surveillance to rise in a very unique context in the world's history, torn apart between a new growing threat to national security and the digital revolution.

### 1. The origins of a growing threat to national security

The 20<sup>th</sup> century is known for its numerous wars all across the world that marked the whole world's history. Besides the three main conflicts (First and Second World Wars and the Cold War), multiple other events happened, such as the Third Afghan War (1919), the Russian, Spanish and Irish Civil Wars (respectively 1917–1922, 1936–1939 and 1922–1923) and tens onward. Since then, the world has been constantly under worldwide conflicts. Even if the Gulf War (1990–1991) happened on Iraq and Kuwait territory, the United Nations took part of the conflict mainly by imposing measures such as trade embargo and military coalition of millions of individuals from 32 countries prepared in case diplomacy and would not be able to solve the conflict.

The implication of States to the conflict became usual, and even the new normality. Nowadays, we expect those States, mainly great powers, to try and regulate conflicts. In the recent events between Ukraine and Russia, countries such as the United States of America and France have made official declarations: the French president *Emmanuel Macron* officially affirmed his support to the Ukrainian

people, and the Commander in Chief of the US military, *Mark Milley*, also spoke about the conflict on the same day (28 February 2022).

This new perspective on interstate conflicts grew from a very peculiar conflict that remodelled the concept of war itself: the Cold War. After the end of the Second World War, a whole new way to deal with an international conflict arose, in which the victory was not given by military forces and weapons, but by information and strategy. If surveillance and spying are very ancient methods to mankind, it was taken to a whole new level in the second half of the 20<sup>th</sup> century.

Intelligence gathering became a priority for both the Soviet Union (Eastern Bloc) and the United States (Western Allies), as a heritage from the nuclear espionage, during the Second World War. Nuclear weapons, considered as one of the most important of all State secrets, were and still are widely coveted. As an illustration, the Manhattan Project was a cooperation between the Allied States, the United States, the United Kingdom and Canada, aiming at developing the nuclear weapon together. The said „atomic spies” would gather information for the sake of the Soviet Union, one of which is known today as *Klaus Fuchs*, a physicist responsible for theoretical calculations to both the early nuclear weapon and the hydrogen bomb.

Espionage between States kept rising and took a major place in the States’ missions. Nuclear espionage, communications interception and military strategy became the centre of the American Central Intelligence Agency, known as the CIA and the Soviet Komitet Gossoudarstvennoï Bezopasnosti (Committee for the State’s Security), known as the KGB.

After the fall of the Soviet Union at the end of the 1980s, the Cold War ended, but States kept their habits of surveillance. A few years later, the September 11 attacks of 2001 turned the world upside down. In the spawn of a single day, the terrorist organisation al-Qaeda planned four attacks on the American ground. Four planes were hijacked mid-air. Two hit the Twin Towers in New York City, a busy working area where thousands of people died and traumatised the whole country. Another plane hit the Pentagon, American headquarters of the US military and defence. The last one was aiming to crash in Washington D.C., the Capital city of the United States and the location of the White House. However, the passengers revolted and it crashed in a field in Pennsylvania. The event is still remembered today as a collective trauma to all Americans that witnessed the events: it was aiming at the destruction of all main aspects of the State: economic, political and military.

It was the first time in History that the United States of America were attacked on their ground by an outsider, as the only previous combat happened in the Civil War. The day

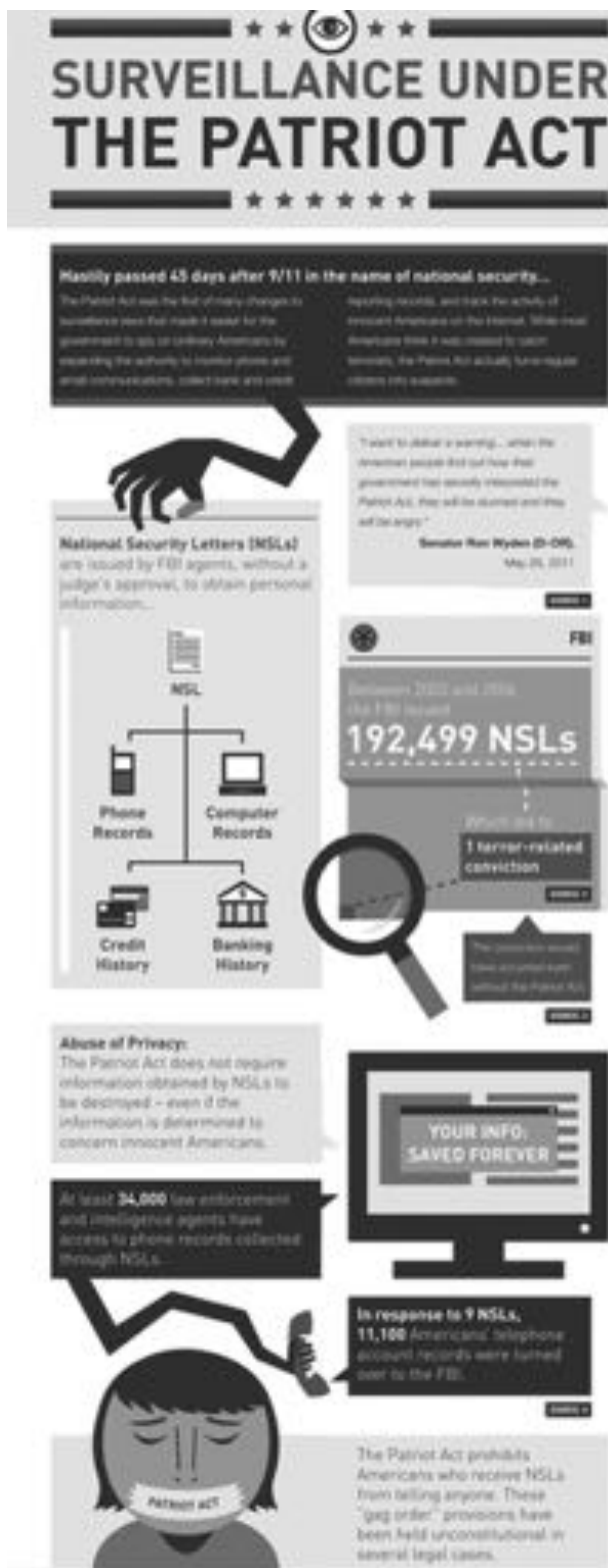
before, the Americans believed they were absolutely safe on their grounds and would not have felt threatened in any way by an attack on their territory, contrary to Europeans who knew hundreds of wars on their grounds, including both World Wars. Many worries and questions were raised then, mainly about security and privacy. As a response, a „War on Terror” has been declared, which led the American defence to build a new program on protection of civilians and destruction of terrorism. The immigration policy was reimagined, and the fear that grew in everyone’s heart led to events of racial profiling and hate crimes towards the Arabic and Muslim communities.

The Act of public law of 26 October 2001, „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”, known as the USA Patriot Act of 2001, has been the legal response to the events of September 11. It amended the Foreign Intelligence Surveillance Act of 1978 and added various new provisions.

Many changes were made, like reinforcement of criminal laws against terrorism to be more strict, but also „enhanced surveillance procedures (Title II)”, „improved intelligence (Title IX)”. The Second Title is meant to give authority to „intercept wire, oral, and electronic communications relating to terrorism” for the purpose of investigations and/or prosecution.

The Patriot Act was voted by the American government to change surveillance laws with the aim to spy on ordinary Americans in the name of national security. Surveillance agencies could then spy on phone and email communications, unnoticed, in the daily lives of their own citizens, as much as many other intrusions of privacy. The use of National Security Letters (or NSLs) was developed: agents of the Federal Bureau of Investigation (or the FBI) could obtain and store anyone’s personal information with no requirement of a judge’s approval beforehand. In three years, from 2003, almost 200,000 were issued, and only one led to a conviction in relation with terrorism, for which the Patriot Act has not been particularly useful (see below: Drawing No 1).

Drawing No 1: Surveillance under the PATRIOT Act.



Source: Surveillance under the PATRIOT Act, ACLU.

Some temporary programs have been very controversial until their disappearance, such as the "business records" provision, which refers to Section 215, "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations". It amends the Title V of the Foreign Intelligence Surveillance Act of 1978 and states by inserting: "The Director of the Federal Bureau of Investigation (...) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents and other items) for an investigation to protect against international terrorism (...)"

In practice, it gives a large margin for the government to ask for anyone that might be involved in terrorist affairs. In 2013, a leakage of documents showed that the government had been collecting phone records of anyone who had a functioning phone, by all companies, under Section 215. *Edward Snowden*, a former computer intelligence consultant, was the source of that enormous leakage of the National Security Agency's documents. Later on, the United States Court of Appeals for the Ninth Circuit ruled that data collection by the NSA, such as exposed by *Edward Snowden*, was illegal on the grounds of the Foreign Intelligence Surveillance Act, and possibly unconstitutional (2 September 2020).

All of those practises are closely related to the recent occurrence of the digital revolution and the new world of possibilities it offers.

## 2. The relationship of surveillance to the digital revolution

Alongside the movement times of the Cold War and the „War on Terror“, the digital revolution also re-shaped the world. With the first computer available to the public being commercialised in 1951 and the development of the Internet's ancestor, Apranet, about twenty years later, the use of digital technology expanded exponentially in both civilian and military aspects, until it became a tool of all our daily tasks. The United Nations specialised agency for ICTs (Information and Communication Technologies) states that about 63% of the world population are connected to the Internet, which represents about 5 billion people.

If there are many ways for the Intelligence agencies of the world to spy on anyone, most of them are via electronic devices and the Internet. Postal services, aerial surveillance, biometric surveillance, infiltration of human operatives, satellite imagery... but mostly computer or telephone surveillance, cameras, social network analysis, data mining and profiling, geolocation devices... are now a part of everyone's daily life.

Since their early years, digital technologies have become the most important source of information for most of us. The Internet is meant to be accessible and easy to use, to all generations. The older generations can use them (if their grandchildren teach them a little), and even toddlers (even though doctors do not recommend it): any member of society has access to it, and the network covers most of the surface of the habitable lands of the world. Such technologies are used daily: when you order food at a restaurant, when you buy a bus or tram ticket, when you call family members or friends, when you play online games, work or study, and even at school.

These technologies have developed mainly during Cold War and have never stopped evolving since then. Military re-

sources are now digitised as well, as much as the Intelligence agencies. In the second half of the 1950s, even before the use of e-mails and computers was democratised, an abuse of surveillance was committed by both the CIA and the FBI, via postal services. The HTLINGUAL program ran until 1973, in which every information outside of a package or envelope was recorded, and allowed to open mails without warrant to read its contents. More than 215,000 pieces of mail were opened this way.

Nowadays, the access to such data has become even easier. Indeed, digital technologies provide opportunities to „hack“ the common individual's data, such as phone or computer records or even credit and banking history. As an illustration, the hacker *Kevin D. Mitnick* explains that all web mail is „cloud based“, which means that, for instance, every email received via Gmail has a copy on Google servers and can be inspected by the hosting company. The official purpose of such measures is to filter out malware. But this way, we, citizens, have no clue why and which emails are read, and neither on what criteria, by the surveillance programs that have a right to claim their data to such companies.

Initially, such data collections via digital tools were meant to prevent criminal activities and protect civilians. It is how programs such as Section 215 of the USA PATRIOT Act expanded their abilities, using the large ocean of data that the Internet is. Indeed, when the common citizen uses online means, they will use online payment, online communication networks and social media such as Twitter, Instagram, Facebook and much more. The digital age allows an easier access to data, but also an easier storage and analysis of such data. Bots can be programmed to pursue a certain mission, and so, less work is required for better results, which facilitate the wide spreading of surveillance to common citizens: intelligence agencies do not have to limit themselves to the known criminal organisations anymore.

Bots are automated software programs: they can achieve repetitive tasks, or predefined tasks according to how their particular algorithm has been coded. It is estimated that about a half of the current activities online are executed by bots. They are used by a wide variety of actors: individuals, companies, hackers, but also for surveillance purposes. Surveillance and security robots in civilian environments can be used for many purposes. They monitor the behaviour, the changes of activities, the habits and all possible information. They can be programmed to execute tasks such as target detection, to keep an eye on an individual, via an automatic system of data collection, filtering and storage.

It can recognise facial features by tracking facial landmark points from any angle, and any facial expression, even if parts of the face are hidden. As an illustration, the Chinese government makes use of this technology to keep a close eye

on its citizens via Closed-Circuit Television, which are cameras disposed all around public spaces, like streets, parks, supermarkets and more. By 2018, it was estimated that over 200,000,000 of such cameras had been installed all over the country, of which a great majority have been installed by the government. It has been recognised that a camera can look for a thousand people at a time, yet Artificial Intelligence experts are working to constantly improve those performances.

全国信标委生物特征识别分技术委, which translates into the National Information Security Standardisation Technical Committee, is meant to enforce mandatory standards for facial recognition in the country. Every person in China in possession of a mobile phone with a registered SIM card has to submit to facial recognition scans, to certify the identity of the holder, which makes them largely easier to track.

A Chinese teacher, *Guo Bing*, employed at the Zhejiang Sci-Tech University, filed what is thought to be the first lawsuit against such practises, as his private data was taken without his consent at Hangzhou safari park, using such a method of facial scanning. Relatedly, the Human Rights activists *Kenneth Roth* stated on a Twitter post, on 1 December 2019 that „China further extends its dystopian surveillance state”, which refers to the system of social score based on your actions and the government’s appreciation: buying alcohol or criticising the government makes you lose points, which can lead to a ban from travel or public shame, and beneficial actions would be rewarded, like participating in charity events.

Cutting edge technologies reinforces the power of surveillance of a State. By reducing the anonymity of people on the Internet, by legally forcing individuals to register their real names when creating accounts online, the artificial intelligence and bots could easily trace individuals’ activities and establish profiles.

Skynet is a surveillance system created in 2005, yet revealed to the public in 2013. At that time, 20,000,000 cameras were already installed in the streets of China’s cities all over the country. The official purpose is to track criminals in a very short time, with cameras being able to recognise anyone in a very short notice, faster than any human intelligence service could ever do. The idea here is to protect nationals, however the use of such technologies have been revealed to go further than tracking of wanted criminals.

Abuses have been revealed: the region of Xinjiang, North West of the country, is the homeland of the Uyghurs community, a Muslim ethnic group. They are forced to give out their biometric data to the State, which includes fingerprints, DNA samples, and voice samples, to allow the government to track them without restriction at any time. Simple actions like growing a beard can then lead them to be interrogated by police and even being put in prison camps.

Other tracking technologies are also used for the purposes of mass surveillance by the Chinese government. Legal norms censor international applications and social media, and force the citizens to choose the „Chinese versions” of those applications. For example, the trendiest social network as of today is „Tik Tok”, developed by the Chinese government itself, but for non-citizens. Their citizens shall use 抖音短视频 (also known as „Douyin”), an application that can be downloaded only if you are permanently geolocated in China. It aims to restrict the foreign influences and users, and allows the government to put into place means of data collection and censorship for the State’s benefit. Other western applications like Facebook, WhatsApp or Uber are being replaced by „WeChat” (that also can serve as a banking service), which facilitates surveillance by the State by gathering all information of individuals in one single application.

What even more facilitates this process for all States is the concept of metadata. Metadata is information of specific features: it is information that provides information for another data. It can be titles of articles, keywords, summaries of e-books, statistical, administrative or legal data. That information create links, and may even reveal new data that has not been directly put online.

The European Court of Justice, in its jurisprudence of „Tele2 Sverige” of 21 December 2016, held that metadata as sensitive information as the content of messages and mails in the perspective of guaranteeing freedoms and rights to the European citizens, mainly in the eye of the right to privacy. They have been listed as „data that makes it possible to trace and identify the source of communication and its destination, to determine the date, time, duration and type of communication, the users’ communication material, as well as locate mobile communication equipment”. This makes massive metadata collection illegal for commercial purposes and the establishment of highly detailed profiles of individuals, but also state’s surveillance collection, even in regard to anti-terrorism protection policies.

That is where a strange idea arises: the protection offered by States to citizens may take away their freedoms, even if the State itself is in charge to guarantee them.

## The paradoxical choice between security and freedoms

That highly developed information creates moral and ethical difficulties that are yet to be solved. On the one hand, there is a need to protect the individual from any threat, counterbalanced on the other hand by the need to guarantee Human Rights to all individuals.

## 1. The need to protect individuals from this threat

The notion of a State is not natural to mankind. The concept has been invented quite recently, when humans started to grow in bigger societies. The first kind of „human” is believed to arrive on earth about 7 million years ago. If our knowledge of their lifestyle is quite limited, since then to the first men of Neandertal (about 300,000 ago), we know that we have always been in groups, living in families of various sizes, but never alone – at least purposefully. Humans gathered and organised themselves in hierarchies, until the first human civilisations, allowed by knowledges such as craft, writing, agriculture, and livestock, in the Fertile Crescent of the Middle-East. Civilisations such as Egyptians were born there and then, and structured themselves in the first systems that would fit our modern concept of a „State”.

States were made for a purpose. The French philosopher, *Jean-Jacques Rousseau*, wrote his ideas on the origins of a State in his work „Du contrat social ou Principes du droit politique” in 1762. He elaborates this idea that men, to protect themselves and improve their living conditions, have agreed to give up a part of their natural freedoms to a man, superior to all else, in exchange for safety, via „pacte social”, an agreement. However, he insists that all should be protected by others, and so give up the freedom that is harmful to others, and only those. It refers, for instance, to the liberty to kill: prehistoric men, without laws and courts to control their actions, would be free to kill someone for their personal gain, and there would be no justice done for his actions: just a never-ending circle of revenge. The Social Contract is the common agreement to give up on this old model of revenge to become a fair and pacifist society within its members.

This abandonment of the idea of „might makes right” (or *kraterocratie*, from the Ancient Greek, meaning that power belongs to the strong ones), led to the current duties of States to protect citizens. But the protection of citizens means to guarantee their rights: if we cannot kill, it is to guarantee the right to life. If we cannot steal, it is to guarantee the right of property. If we cannot discriminate, it is to guarantee equality.

Modern societies such as ours have evolved a lot since those first civilisations. The possibilities to attack someone, to violate someone else’s rights have become wider, notably since the digital revolution. Governments have to expand their protection to the digital world: it is unimaginable that a State would have a criminal policy, but no laws concerning cyber criminality. The Internet is a shared space, in a similar way that a street is, in this regard. For instance, in a country where drugs are illegal, it should not be possible to buy any online. Otherwise, dealers and clients would just need to code an online shop to go around all the criminal laws. This would imply that any crime is not punishable if committed

online, which would not guarantee rights of the individual at its fullest, causing the State to automatically fail at its mission of protection of civilians.

It is following this objective that the European Union adopted a Regulation (the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC „Data Protection Directive”), known as the General Data Protection Regulation 2016/679, or GDPR, implemented in 2018. Its first article states the subject-matter and objectives of the regulation: „1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data”.

It hence recognises the Digital tools as potentially dangerous, and the necessity of a legal framework so as to guarantee the citizen’s free and fair use of those means. The European Union aims at protecting citizens from online criminality, but also to protect the individual’s personal data. Data processing requires the individual’s explicit and aware consent, unless it is in their vital interests, or the compliance with legal obligations, for instance.

As an illustration, medical data is considered to be one of the sensitive personal information that should not be forced to be revealed without explicit and informed consent. However, during the Covid pandemic, some countries required a proof of a negative PCR test or vaccine against the disease. As an illustration, the French government established limitations on the access to some places available to the public, such as cinemas, museums, shops or restaurants. „Le pass sanitaire” was a QR-code given after being vaccinated in a specialised establishment that would be valid after two injections, currently turning into three injections, of the vaccine. Implemented in June 2021 and still in place up to date, this was a very controversial measure. Citizens are required to register their QR-code into their phone via an application developed by the government, „Tous Anti-Covid” (which translates into „together against covid”). Then, anytime they enter a public place requiring the presentation of the vaccinal pass, they have to show their QR-code at the entrance, where it would have been checked by a security guard, or in some cases an employer.

The obligation to disclose such personal data has been justified as a temporary measure that is not meant to last in time, and serves national security as it aims at preserving public health. It allows the government to enforce its meas-

ures. In the controversy that it leads, the resistance to such measures, even in the name of national health, security, and public order, comes from the highly sensitive nature of the data. Other than just disclosing your personal information, you also give out your position, where you were and with whom, as you register your QR-code that contains all that information.

The State's objectives are to preserve national integrity, safety of its citizens, and its fundamental interests. For a State to last in time, it needs tranquillity and trust between the government and the individuals. Covering the nation's interests online is just as fundamental to guarantee those two feelings as any other policy. For a national unity, there is an absolute need for the State to protect citizens in all aspects of their lives. As individuals spend more and more time online, as much as share more and more data online, sometimes without even realising it, a State cannot be forbidden to have a presence online for defensive and protective means, this would simply not be adapted to our times.

States must have a possibility to keep an eye on what is happening online, as much as to react to such things. The question, however, is where the limit of this ability should be. When is it too much freedom and too little security? And, on the other hand, when is it too much security and too little freedom?

To grant effective protection, new rights were granted to the individuals making use of digital technologies. The fundamental rights of data subject has been recognised as such: the right to access to information, the right to access to the data itself, the right to rectification of your data, the right to be forgotten (which implies the right to delete information about yourself), and the right to withdraw consent at any moment. To guarantee that protection does not overrule freedoms, these new rights have to be guaranteed by the State, as any other right.

## 2. The need to guarantee the individual's Human Rights

The European Court of Justice has shown opposition to the mass collection and storage of data from online connections and phone use by States. On 6 October 2020, it held such a decision, rejecting the possibility for States to require Internet Service Providers, or ISPs, to give out the data and metadata of their clients, even for purposes of justice and surveillance. More precisely, it was held that States could not impose „une obligation généralisée et indifférenciée”. This means that it is not possible to imagine a general legal norm imposing all ISPs to share their data to the States at all times, from all of their clients and all of their communications.

It was deemed that measures such as those taken by France, Belgium or the United Kingdom (that latter still being

a member of the European Union back then) in the context of their anti-terrorism policies were contrary to European law. The collection and storage of such sensitive information have to be limited and based on legitimate interests: all citizens cannot have their information collected at once, according to the General Advocate *Manuel Campos Sanchez-Bordona*. Targeted and precise surveillance does not fall under the scope of the restrictions imposed by the State. They attempted to contest this decision, on the basis that according to the Treaty of the European Union, national security is the competence of Member States and Member States only: it is exclusive and the European Union should not be entitled to restrict its possibilities.

In a more recent opinion of 18 November 2021, the same Advocate General, *Manuel Campos Sanchez-Borbona*, added that the „general and indiscriminate retention of traffic and location data relating to electronic communications is permitted only in the event of a serious threat to national security”. The element of a serious threat to national security is recognised as the only possible justification, as a strict condition, to mass surveillance of individuals by the State. It would be possible to exercise such measures in cases where it is absolutely required so as to guarantee the safety of the individuals, in which case it is recognised as a proportionate and adequate response to the threat.

It cannot be understood that this scope widens, as it implies interference with basic Human Rights guaranteed by most Human Rights Charters across the World, notably the right to privacy. The consequences on the deprivation of the right to privacy, guaranteed by article 8 of the European Charter on Human Rights, has consequences on other Human Rights. They are fundamentally related to each other, and the loss of one may result in the loss of all. In this case, it might limit the rights to freedom of expression and opinion, which impacts democracy as much as the rule of law itself, and their safeguarding.

*Murray Gleeson*, a former Chief of Justice in Australia, defined what makes data private. He established a simple test to determine any information as such: „The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private”. Hence, if it is generally accepted that the information is usually not shared with others, except for close relatives or friends, the data must be considered and treated as private. People might want to keep their data private for many reasons: the need for intimacy, the social pressure that may ensue, or the fear that such data may be used against oneself.

In the case of collection by a State, the use against oneself would be the main scare for individuals. One of psychology's principles, known as the Observer Effect, explains that there is a „self-editing effect”. It implies that the individual

would automatically filter their words if they are aware of a possibility to be recorded by a State, even if the said State is not actively doing so. This tends to be even more noticeable when the said individual has political or cultural opinions that vary from the usual norm amongst the citizens, and the State policies. As an illustration, we may use the anachronist example of the creation of democracy. If *Cleisthenes* was being potentially watched by a conservative intelligence system, he may not have reformed the political regime of Athens in the year 507 B.C., and the *demokratia* would never have been implemented. Society would not have been able to evolve, and in that scenario, we probably would not live in a democracy today.

In those cases, misuse of private data may be the source of worry. In a State like China, citizens are taking disproportionate risks by criticising the government. They fear for their life and restrain their will to speak up about their opinions, beliefs, in case they might be in discordance with the government policies, as it may detain that information to sentence every attempt to contradict the measures in place. This limits the diversity of ideas in a society, and causes the citizens, mostly younger children, to automatically agree with the government by lack of exposure to new and different ideas. How can Chinese people reject the exponential development of cameras equipped with artificial intelligence if they have been told that it helps with keeping the country safe, but have never been told what risks might be the cause of it? What downsides are to be expected? In the long run, it limits the possibility itself to think for themselves, to develop a very own and personal vision, but conforms all individuals into one path of thought.

Article 8 of the Convention of Human Right, on the right to respect for private and family life, states that „1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

These framed limitations of article 8 are closely related to the need for protection of private data: self-determination of the use of our personal information is the key to preserving all rights required in a democratic society led by the rule of law, which the State is bound to safeguard. The European Court of Human Rights held in two General Court jurisprudences, *Centrum för rättvisa v. Sweden* 2021 and *Big Brother Watch and Other v. The United Kingdom* 2021, that the existence of secret data surveillance deprives of the rights guaranteed by article 8 as it is impossible for the individual to challenge the

act and they are not aware of what can be performed with their own data. The mere existence of such a policy can lead to a violation of the article in certain conditions as stated in *Roman Zakharov v. Russia* 2015 (§ 171–172). There is a need for supervision of the relevant national judicial authorities, to prevent abuses and misuses. National authorities cannot have full and incontestable discretion in determining what system of surveillance is required, and its extent.

Surveillance is legal and tolerable as long as it is strictly necessary to preserve democratic institutions, and remedies shall be available to sentence abuse and misuse of surveillance. In the case of *Weber and Saravia v. Germany*, the Court held that data must be „used only for the purpose which had justified their collection” (§ 150) and that „in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (...). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law” (§ 106). In this regard, the Court found to be in violation of the article regarding the recording of a conversation by a long distance radio device during a police operation without procedural safeguards<sup>3</sup> or the systematic collection of data of security services targeted on particular individuals even in public places<sup>4</sup>.

Even if article 8 of the Convention is the most obvious regarding the risks to Human Rights caused by mass surveillance, it is far from the only one: for instance, Article 6, on fair trial, also reveals potential limits to the possibility of mass surveillance. In *Lopez Ribalda and Others v. Spain* 2019, the Grand Chamber of the European Court of Human Rights held that the use of evidence based on data obtained in violation of article 8 and/or in violation of domestic law, the trial must be considered as unfair and breaching article 6 of the convention, as it may interfere with the defence rights to the parties, and the opportunity to contest the authenticity of the evidence has to be ensured as well. Nuances shall be brought, as evidence rules for civil and criminal proceedings vary<sup>5</sup>.

The complexity of the application of mass surveillance is its paradoxical consequences: it opposes the security to freedom, two fundamental elements to a fair and safe democratic

<sup>3</sup> *Bykov v. Russia* 2009.

<sup>4</sup> *Peck v. United Kingdom* 2003.

<sup>5</sup> See: Article 6 of the European Convention on Human Rights.

society, as neither of them shall be undertaken by the other. It enhances a need to search for balance, an equilibrium that could guarantee both to all individuals.

## The search for balance between security and freedom

In the context of mass surveillance, security and freedom have a rather conflictual relationship. First, it is necessary to understand the various interests that justify security and/or freedom as fundamental in our societies. Secondly, there is the need to nuance an apparent opposition of both concepts that seems to counterbalance each other, as if a choice had to be made when our democratic societies need them both as much. We shall aim at the coexistence of those two concepts, even though they seem opposites, they do not have to be contradicting each other.

### 1. A divergence of interests to protect

As *Arnold Wolfers* said in 1952, „the term ‘security’ covers a range of goals so wide that highly divergent policies can be interpreted as policies of security”. Indeed, the word security may imply the protection by the State of individuals, institutions, economic powers, territorial integrity... All threats imaginable must be ward off by the State: it is nowadays the State’s role to keep individuals safe from murder, discrimination, food security, but also Human Rights violation, terrorist attacks, cybercrime and so much more.

This may be done via the American National Security Act of 1947, the German White Papers („Zur Sicherheit der Bundesrepublik Deutschland und zur Entwicklung der Bundeswehr”), the Chinese White Papers, such as the one from 2019 which reinforces its strategic partnership with Russia, the French White Papers of 1972 which aims at reducing the proliferation of nuclear weapons, or even the Japanese with constitutional norms and the National Defence Program Guidelines.

All States have policies of national security and defence. However, according to their very own values, expectations, means and beliefs, those policies may have their priorities at highly divergent points. Indeed, due to their particular culture and history, all States have different problems to face while protecting their country, and this applies just as much to cybersecurity and intelligence. During the 2000s, countries such as the United Kingdom, the United States of America or France had their national security centred on the fight against terrorism, while Japan was more focused on the area of the Pacific region of Asia, where tensions were rising in China on internal divisions such as the issues of Taiwan and Xinjiang.

States have different characteristics, which have been analysed in *Buzan’s* ‘People, States and Fear’, book of 1991. The

author focuses his work on two fundamental factors: the power of a State, notably its military abilities in international conflicts, and its socio-political cohesion, which refers to the nation’s stability and unity of its people. This model shows that a State with weaker military forces and low social cohesion will be more vulnerable to most types of threats. A State with a weak military power will only be vulnerable to international threats and invasions, while a State with no socio-political cohesion will be the most vulnerable to internal threats such as civil revolts. All those States will not have the same idea of potential threats, and of national security and measures to take. In the eyes of mass surveillance, this implies diverse possible uses of such measures, as much as different needs and levels of implications demanded by the States (see below: Tables No. 1 and 2).

**Table 1.** Vulnerabilities and Types of States (taken from *People, States, and Fear* (1991))

| Weak  |        | Socio-political Cohesion                     |                                                                                                    |
|-------|--------|----------------------------------------------|----------------------------------------------------------------------------------------------------|
|       |        | Strong                                       |                                                                                                    |
| Power | Weak   | Highly vulnerable to most types of threats   | Particularly vulnerable to military threats                                                        |
|       | Strong | Particularly vulnerable to political threats | Relatively invulnerable to most types of threat (less inclined to characterize issues as military) |

**Table 2.** Cyber Vulnerabilities and Types of States

| Weak  |        | Socio-political Cohesion                                                                                |                                                          |
|-------|--------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
|       |        | Strong                                                                                                  |                                                          |
| Power | Weak   | De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities | DDOS and other major attacks on critical infrastructure* |
|       | Strong | De-stabilizing political actions in cyberspace                                                          | Criminal activities in cyberspace                        |

\*A distributed denial of service attack, or DDOS, occurs when many computers, usually surreptitiously controlled, are used to inundate a web server with requests and cause it to become overwhelmed to the point that service is denied.

Source: Tables extracted from *B. Buzan, People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 1991.

The first type of a State will be worried about most types of threats that may be foreseeable in cyberspace. The second type will mostly be worried on issues of attacks on the Internet infrastructure, international terrorism and interstate conflicts, while the third will be more focused on politically destabilizing forums, for instance. Surveillance may be used as a tool to protect from each of those threats, by making different uses of the same abilities intelligence agencies have. The objective leading mass surveillance measures will be strongly connected to the extent and consequences on liberties of such surveillance.

This emphasises that even if the security brought by mass surveillance may infringe fundamental liberties and freedoms and even Human Rights, there can be hundreds of ways to link those two notions, and how they interact.

## 2. The coexistence of opposite but not contradicting ideas

As elaborated earlier, the notions of freedom and security are conflictual when it comes to mass surveillance. In this context, data collection interferes with freedoms it is trying to protect. Mass surveillance and data collection by the States aims at reinforcing national security and guaranteeing the safety of each individual. On the other hand, not permitting the State to have such surveillance abilities would not guarantee everyone's security, even if that would not interfere with freedoms.

Those impacts will mainly depend on the means and ways of mass surveillance, data collection and storage. The United States of America and China both have mass surveillance programs. However, it does not have the same consequences in both countries: in China, each individual's single actions are evaluated and analysed, and so every word they say may be prejudicial to them which leads to a fall of the liberties of expression, freedom of opinion and rights to a private life. In America, mass surveillance collects a lot of data and mostly metadata, in the purpose of finding actual threats to the nation, via very intrusive means. This reveals that even if this violates the right to privacy, it does not in all cases lead to the fall of democracy and liberty of thought.

The concepts of security and freedom do not have to be opposed to each other. Today, in the context of mass surveillance, they surely are. However, it might be possible to think of a method of surveillance that would not infringe liberties at all, including the right to privacy. We have to keep in mind that most measures in western countries were taken in the heat of the War on Terror, mostly as emergency measures and responses to the attacks of al-Qaeda and other such organisations: the USA PATRIOT Act 2001 was adopted just a few weeks after the events of September 11.

In all of history of humanity, first steps have always been halting and perfectible. The mass surveillance measures were taken in the urgency of a peculiar context and the sudden rise of terrorism, interstate conflicts and digital revolution. All those new threats and tools were still an unknown field, and to predict the consequences of such new actions may have been a real challenge.

However, today might be the time for a „post-project analysis”, the time to reconsider the actions taken as much as their consequences, notably on Human Rights. To re-think previously taken measures and adapt them in a more rational way, with a deeper analysis of what it costs and what it allows. Nowadays, we have the hindsight that no one had thirty to twenty years ago. We have more concrete ideas of how digital tools may be used and their consequences on health, security, and liberties<sup>6</sup>.

Security does not have to mean we give up on Human Rights. As *Jean-Jacques Rousseau* meant it, the role of the State is to bring security to the individuals, because safety is what allows them to be free. Inherently, security is a condition to liberty, and should not enslave it. The problem is not that mass surveillance keeps us safe, it is that the ways and the tools used in the policies of mass surveillance sacrifice liberties and human rights in the name of national security. This, however, does not mean coexistence is not possible at all: just not on our modern and current use of these tools. There are other ways to protect that we may use instead.

## Conclusion

We may imagine a close future in which the States would gather and discuss those issues, and work together in the aim of mass surveillance and its current effects on Human Rights. A State has to protect its citizens from threats, even online. Rights and obligations shall coexist in cyberspace so as to ensure Human Rights, but without going into extreme ways that would cost the loss of Human Rights as well.

Here, there is a question of balance of values and considerations. New legal norms and regulations shall be taken in the light of the hindsight we now have. It is possible to keep an eye on people without taking away their right to privacy and other liberties away from them.

Surveillance of population may be possible without storing huge amounts of data and metadata to sort out information in a more intelligent and balanced way that would

<sup>6</sup> P. Toomey, A. Gorski, The Privacy Lesson of 9/11: Mass Surveillance is Not the Way Forward, ACLU 2021: „By reining in mass surveillance, Congress can begin the process of righting the privacy harms of the last twenty years. And looking toward the future, Congress can help ensure that the next generation of Americans are able to speak and associate freely, without fear of unwarranted government scrutiny”.

guarantee all Human Rights and security at the same time. Working methods of intelligence agencies have to be revised in that perspective so as to ensure a safe world for all, while preserving both State's and individual's interests.

The main obstacle would be the compliance of the States, but all great changes in History came step by step. Every State has a unique policy and unique interests to defend as well, and so a generalised movement would require a lot of work

of understanding of each other and communication, in the abstract of all political or diplomatic tensions there might be. Such great compliance has been seen before, notably with the establishment and recognition of the United Nations: it is not impossible when common interests are shared, such as global and stable peace. Change, even for the better, requires work and dedication. It is a progressive mechanism, an action for the future.

**Keywords:** National Security, Digital Age, Private Data, Surveillance, Human Rights, Privacy, Democracy.



# SZKOLENIA PRAWNICZE

*Rozwijaj karierę z zaufanym partnerem*



#### Doświadczeni prelegenci

– wieloletni praktycy i pasjonaci w zakresie prawa



#### Najwyższy poziom merytoryczny

– aktualne i praktyczne analizy zmian w prawie



#### Gwarancja rozwoju

– udział w szkoleniach skutkujące  
nauką kompetencji zawodowej



#### Pakiet korzyści

– specjalistyczne publikacje oraz dostęp do Systemu Legalis  
stworzył wiedzę zdobytą podczas szkoleń



#### Punkty szkoleniowe

– wymagane w ramach doskonalenia  
zawodowego przez KTD, ORA, OIRP

**beckakademia**

więcej na: **akademia.beck.pl**

# Oprogramowania oparte na sztucznej inteligencji w sądach na całym świecie: praktyka, perspektywy i wyzwania mające znaczenie dla Węgier i Europy Środkowej<sup>1</sup>

Kinga Kálmán<sup>2</sup>

Laura Olga Kiss<sup>3</sup>

Kitti Mezei<sup>4</sup>

Boldizsár Szentgáli-Tóth<sup>5</sup>

Na przestrzeni ostatnich kilku lat na międzynarodowym polu naukowym są prowadzone dyskusje na temat możliwości zastosowania sztucznej inteligencji w sądach z udziałem przedstawicieli wielu dyscyplin. Nie inaczej jest na Węgrzech. Antagonistyczne poglądy utknęły jednak właściwie na poziomie uogólnień opartych na teoretycznych punktach wyjścia, a nauki prawne poczyniły dotychczas niewiele namacalnych ustaleń w kwestii tego zjawiska, głównie ze względu na brak konkretnego doświadczenia praktycznego. W niniejszym opracowaniu, po sprawozdaniu z obecnej sytuacji na Węgrzech, autorzy przeanalizują, jakie rozwiązania funkcjonują już za granicą i co można powiedzieć o ich skuteczności oraz wpływie na procedury. Ma to na celu przybliżenie tej nowoczesnej technologii, jaką jest oprogramowanie oparte na sztucznej inteligencji czytelnikom, a więc praktykującym sędziom, przedstawicielom innych zawodów prawniczych, jak również wszystkim osobom poszukującym teraz lub w przyszłości pomocy prawnej albo po prostu zainteresowanym tym, jak za jakiś czas będą wyglądały sądy. Tak odległe pozornie procesy nie ominą ani Węgier, ani całego regionu, dlatego istotne jest, aby zająć się tą gałęzią nowoczesnej techniki sądowej.

## Uwagi wstępne

Wielokrotnie, nawet w środowisku prawników, pojawia się wiele błędnych wyobrażeń na temat roli sztucznej inteligencji w sądzie. Licznie też reprezentowane są przewidywania, że upowszechnienie się tych narzędzi może podważyć dotychczasowy system gwarancji prawa do rzetelnego procesu sądowego i postawi strony sporu w trudnej sytuacji<sup>6</sup>. Jednocześnie równie często wyrażany jest pogląd nastawiony wyłącznie na efektywność, który zastosowanie sztucznej inteligencji uznaje za cel nadrzędny, nawet za cenę – przynajmniej w pierwszym okresie – realnego ryzyka naruszenia praw podstawowych człowieka, takich jak prawo do rzetelnego procesu sądowego<sup>7</sup>. Niewiele jest jednak prac, które starają się uchwycić nowe technologie takimi, jakie są naprawdę, pokazując ich praktyczne zastosowanie ze wszystkimi ich zaletami i wadami.

Z powyższych względów konieczne jest rozwianie niektórych elementarnych nieporozumień związanych z legalną pracą sztucznej inteligencji<sup>8</sup>. Z jednej strony, na obecnym poziomie rozwoju technologicznego, jesteśmy bardzo daleko od wizji sędziego-robota – póki co nie można posłużyć się żadnym przykładem, który dowodziłby chociażby czegoś podobnego. W rzeczywistości chodzi o to, że w technologiach stosowanych w administracji wymiaru sprawiedliwości są instalowane oprogramowania oparte na sztucznej inteligencji, która w określonych sytuacjach potrafi samodzielnie podej-

mować decyzje albo przynajmniej stworzyć niezależny tok myślenia, jak również systematycznie uczyć się na błędach. Dla strony procesu fizyczna zmiana na sali sądowej spowodowana zastosowaniem sztucznej inteligencji jest więc ledwo zauważalna, natomiast cały mechanizm decyzyjny faktycznie ulega znacznej transformacji.

Z drugiej strony, sztuczna inteligencja obecnie – poza kilkoma mocno wątpliwymi przykładami z Chin – uczestniczy w pracach sądowych jedynie pod ścisłą, stałą kontrolą człowieka, a zatem nie ma mowy o tym, żeby technologia przejęła rolę człowieka<sup>9</sup>. W tej chwili mówimy raczej o na-

<sup>1</sup> Studium przygotowano w ramach przetargu NKFIH Nr 138965 oraz Narodowego Laboratorium Sztucznej Inteligencji przy wsparciu Ministerstwa Innowacji i Technologii oraz Narodowego Biura Badań, Rozwoju i Innowacji.

<sup>2</sup> Asystent naukowy, Centrum Nauk Społecznych, Instytut Nauk Prawnych, Budapeszt.

<sup>3</sup> Doktorant na Narodowym Uniwersytecie Usług Publicznych w Budapeszcie.

<sup>4</sup> Badacz, Centrum Nauk Społecznych, Instytut Nauk Prawnych, Budapeszt.

<sup>5</sup> Badacz, Centrum Nauk Społecznych, Instytut Nauk Prawnych, Budapeszt.

<sup>6</sup> M. Dymitruk, The right to a fair trial in automated civil proceedings. In: Masaryk University Journal Of Law And Technology 2019, Nr 1, s. 27–44.

<sup>7</sup> A. Roth, Trial by machine, Georgetown Law Journal 2016, Nr 5, s. 1–48.

<sup>8</sup> C. de Saint Laurent, In defence of machine learning: debunking the myths of artificial intelligence, Europe's Journal of Psychology 2018, Nr 4, s. 734–737.

<sup>9</sup> M.U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, Harvard Journal of Law & Technology 2016, Nr 2, s. 1–48.

rzędziach, które na różne sposoby wspomagają pracę sądu<sup>10</sup>, a do których dane wprowadzone są przez ludzi, proces decyzyjny uruchomiany jest przez ludzi, a decyzję, w jakim stopniu będą opierać się na danych, analizach i dokumentach dostarczonych przez sztuczną inteligencję, podejmują również ludzie (członkowie sądu)<sup>11</sup>. Nie można wykluczyć, że na późniejszych etapach rozwoju technologicznego trzeba będzie inaczej podejść do tego problemu, ale na razie można mówić raczej o podboju sądów przez nowoczesne technologie, a nie o całkowitej transformacji logiki orzecznictwa czy też przeniesieniu władzy sądowniczej na maszynę<sup>12</sup>.

Poniżej przedstawiony najpierw zostanie krótki przegląd sytuacji na Węgrzech, a następnie te aplikacje zagraniczne, które są istotne z punktu widzenia niniejszego opracowania w podziale na trzy kategorie – według ich roli w pracy sądowej. Na początek omówione zostaną programy, które służą pomocą na pewnym etapie pracy sądowej, np. wyszukiwają w orzecznictwie precedensy i na tej podstawie przeprowadzają analizę. Następnie omówione zostaną rozwiązania, które przygotowują propozycje pewnych orzeczeń, a nawet wyroków, jednak decyzja co do ich wykorzystania pozostaje w gestii złożonego z ludzi sądu, który może te sugestie nawet zignorować. Na koniec uwaga zostanie poświęcona narzędziom, które wyręczając sąd, mogą podejmować samodzielne decyzje np. o dopuszczalności wniosków. Zastosowanie sztucznej inteligencji w sądach to wyzwanie na dziś<sup>13</sup>, a sąd, w którym wyroki wydaje sztuczna inteligencja, to dopiero kwestia przyszłości<sup>14</sup>.

## Dotychczasowe etapy wdrażania sztucznej inteligencji w węgierskim sądownictwie

W węgierskim sądownictwie nie odnotowano jeszcze innowacji podobnych do przedstawionych poniżej zagranicznych przykładów. Jednak nawet na Węgrzech w ostatnich latach można zauważyć drobne zmiany w zakresie cyfryzacji administracji sądowej, który to proces w 2018 r. otrzymał nazwę e-Sąd. E-Sąd obejmuje wszystkie aplikacje i narzędzia IT dostępne dla sędziów, klientów i pracowników administracji sądowej. Można podzielić je na takie, które wspomagają pracę sędziego lub konkretnie proces orzekania, i takie, które wspierają klientów. Do tych pierwszych należą m.in. programy do automatycznego wypełniania formularzy i akt sądowych, aplikacje do monitorowania terminów i przedawnień albo programy do redagowania, publikowania i anonimizacji orzeczeń sądowych<sup>15</sup>.

Najważniejszym elementem większości systemów sądowych jest oprogramowanie dla administracji (na Węgrzech pod nazwą BIIR: Sądowy Zintegrowany System Informatyczny), które jest jednocześnie rejestratorem i rejestrem akt

oraz, w wąskim zakresie, służy wspomaganie pracy grupowej. W sądach węgierskich podstawowe dane dotyczące spraw sądowych są lub będą doręczane przez elektroniczny system informacyjno-ostrzegawczy sądów (BETFR), podczas gdy kompletne akta, czyli elektroniczny wgląd do akt sądowych, zapewnia lub będzie zapewniał system e-dokumentów<sup>16</sup>. Obecnie oprogramowanie do rozpoznawania i nagrywania mowy służy sędziom do automatycznego zapisania materiału dźwiękowego bez udziału człowieka, co może znacznie skrócić czas administracyjny i proceduralny.

Utworzone zostały elektroniczne interfejsy do kontaktu z sądami i wymiany informacji. W większości postępowań sądowych przedstawiciele prawni lub osoby prawne mogą składać wnioski o wszczęcie postępowania wyłącznie drogą elektroniczną. W ten sam sposób komunikuje się również sąd.

W ciągu ostatnich lat w węgierskich sądach zainstalowano również system do zdalnych przesłuchań (system wideokonferencji), który nadaje się też do wykonania zapisu audio-wideo w salach sądowych oraz przesyłania tych nagrań.

Ogólnie rzecz biorąc, cyfryzacja w sądach węgierskich jest obecna, ale nie w takim stopniu jak w niektórych przykładach zagranicznych przedstawionych w badaniu. Nie ulega wątpliwości, że już te rozwiązania mogą wspomóc pracę sędziów, przyspieszyć i usprawnić niektóre procedury oraz ułatwić korzystanie z prawa do drogi sądowej<sup>17</sup>. Brakuje im jednak fakturowy sztucznej inteligencji – chociaż bowiem węgierskie oprogramowania potrafią spełnić wiele funkcji, które są również istotne dla systemów opartych na sztucznej inteligencji, to jednak technologie oparte na uczeniu maszynowym nie zyskały jeszcze na Węgrzech popularności.

Dopóki sytuacja się nie zmieni, dopóty można mówić tylko o cyfryzacji i automatyzacji pracy sądów, a o sądowym zastosowaniu sztucznej inteligencji już nie. Jednak znane obecnie i opisane poniżej bardziej szczegółowo zagraniczne przykłady mogą wskazać Węgrom i innym krajom regionu kierunek rozwoju pod kątem tego, jak można w pełni wykorzystać nowoczesne technologie w pracy sądu, poprawiając jej

<sup>10</sup> Z. Zódi, The code of AI and human laws, *Acta Universitatis Sapientiae Legal Studies* 2018, Nr 2, s. 253–268.

<sup>11</sup> R.M. Re, A. Solov-Niederman, Developing Artificially Intelligent Justice, *Stanford Technology Law Review*, Stanford 2019, s. 242–290.

<sup>12</sup> T.J. Buocz, Artificial intelligence in court. legitimacy problems of ai assistance in the judiciary, *Artificial Intelligence in Court* 2018, Nr 1, s. 41–59.

<sup>13</sup> T. Sourdin, Justice and technological innovation, *Journal of Judicial Administration* 2015, Nr 2, s. 96.

<sup>14</sup> T. Sourdin, Judge v robot? Artificial intelligence and judicial decision-making, *University of New South Wales Law Journal* 2018, Nr 4, s. 1114–1133.

<sup>15</sup> A. Osztoivits, Sądy cyfrowe a prawo do sprawiedliwości – szansa czy zagrożenie? *Prawo węgierskie* 2020, Nr 11, s. 627–628.

<sup>16</sup> Z. Zódi, Sądy i technologia, *Monitor sądowy* 2020, Nr 1, s. 6 i 8.

<sup>17</sup> A. Osztoivits, Sądy cyfrowe a prawo do sprawiedliwości – szansa czy zagrożenie? *Prawo węgierskie* 2020, Nr 11, s. 627–628.

efektywność i utrzymując jednocześnie aspekty gwarancyjne. Dotychczas powołano tylko kilka zespołów roboczych do promowania tego zagadnienia. Można tu również wspomnieć o badaniach A. Nagy<sup>18</sup>, ale intensyfikacja profesjonalnej dysputy pozwala przypuszczać, że wkrótce przyniesie ona wyniki w postaci praktycznego postępu i poszerzenia fachowej literatury.

## Narzędzia wspierające pracę sądów, a w szczególności ich działalność administracyjną

### 1. Oprogramowanie wspierające analizę orzecznictwa, baza orzeczeń prowadzona przez sztuczną inteligencję

Wracając do przykładów międzynarodowych, które można wykorzystać jako punkt odniesienia, w pierwszej kolejności należy zwrócić uwagę, że szczególnie w krajach *common law*, takich jak Stany Zjednoczone i Wielka Brytania, zebranie i znalezienie właściwych orzeczeń sądowych w danej sprawie jest niezwykle ważne, ponieważ tam wcześniejsze wyroki sądowe mają kluczowe znaczenie. Jednocześnie w kontynentalnych systemach prawnych, a tym samym i na Węgrzech, coraz ważniejsze staje się poznanie orzecznictwa i, w razie potrzeby, odwołanie się do niego we wnioskach.

Taka działalność – analiza orzecznictwa – to zwykle zadanie, które wymaga poświęcenia długich i wartościowych godzin pracy, mimo że praca odbywa się już prawie wyłącznie z internetowymi bazami danych.

Analiza orzecznictwa, oprócz odpowiednich orzeczeń sądowych, obejmuje również analizę uzasadnienia legislacyjnego wymaganego przez prawo, stosownej literatury i komentarzy, co także jest czasochłonne. Chociaż oznacza to dodatkowe zadanie zwłaszcza dla stron procesowych i ich przedstawicieli prawnych, jednak konieczne jest, aby również sądy analizowały własne orzecznictwo, w szczególności zaś orzecznictwo sądów apelacyjnych.

Programy oparte na sztucznej inteligencji ułatwiają właśnie te zadania.

#### 1.1. Stany Zjednoczone, Wielka Brytania: LexisNexis, Alexsei, Westlaw, AnyLaw

Na obszarach anglosaskich inicjatywy państwowe na rzecz cyfryzacji prawa są znikome – kluczową rolę w sektorze prawnotechnologicznym odgrywają prawie bez wyjątku firmy prywatne, które świadczą swoim użytkownikom usługi nastawione głównie na zysk, oparte na subskrypcji. Większość z nich rozwinęła się z internetowej prawniczej bazy danych w korporacyjnego giganta, poszerzając swoje usługi.

Produkty firmy CALR (*Computer-Assisted Legal Research*<sup>19</sup>) pojawiły się w pierwszych latach XXI w. a wśród nich najbardziej prekursorski był LEXIS, jak również Westlaw.

Następca LEXISa, LexisNexis<sup>20</sup>, jedna z najpopularniejszych obecnie prawniczych baz danych, wykorzystuje najnowsze technologie, takie jak sztuczna inteligencja, uczenie maszynowe, generator tekstu, jak również narzędzia do eksploracji tekstu i wizualizacji. Baza danych opiera się na ponad 83 miliardach aktów prawnych i orzeczeń sądowych, ponad 40 000 artykułów i danych z rejestru przedsiębiorstw dla milionów firm<sup>21</sup>. Zapewnia kompleksowe usługi, a najważniejsze z punktu widzenia naszego opracowania funkcje to:

- a) Lexis Answers,
- b) Lex Machina,
- c) Ravel View.

#### 1.2. Odpowiedzi w kwestiach prawniczych

Pośród usług LexisNexis można wyróżnić oparty na sztucznej inteligencji program Lexis Answers<sup>22</sup>, który podaje krótką i wiarygodną odpowiedź na pytanie postawione przez użytkownika, bez konieczności wyszukiwania przez niego słów kluczowych. Zasadniczo wygląda to tak, że użytkownik zadaje swoje składające się z kilku słów pytanie (input), niczym pytanie skierowane do innej osoby, swego rodzaju przedstawiciela prawnego, po czym program przeprowadza wyszukiwanie w swojej bazie danych, a następnie, po dokonaniu oceny, wyrzuca „najlepszą odpowiedź” w postaci Lexis Answers Card, czyli karty odpowiedzi (output). Karta odpowiedzi nie tylko powołuje się na konkretny akt prawny, ale zawiera nawet jego tekst (a właściwie go cytuje), przyspieszając tym samym cały proces. Dzięki uczeniu maszynowemu, im więcej wyszukiwań dokonują użytkownicy na interfejsie, tym dokładniejsze odpowiedzi może dostarczyć Lexis Answers.

Podobne usługi oferuje działający również w zakresie prawa anglosaskiego Alexsei<sup>23</sup>, będący wspólnym produktem intelektualnym zespołu prawników i ekspertów w dziedzinie sztucznej inteligencji. Na zadane przez użytkownika prawnicze pytanie program przygotowuje memorandum, które składa się z trzech głównych części:

- a) pytania zadanego przez użytkownika i podanych przez niego faktów;

<sup>18</sup> A. Nagy, Znaczenie i możliwości wykorzystania sztucznej inteligencji i cyfryzacji w służbie wymiaru sprawiedliwości, *Monitor prawny w Miskolcu* 2020, Nr 3, s. https://www.mjsz.uni-miskolc.hu/files/13829/13\_nagyadrienn\_tordelt.pdf (dostęp z 1.1.2021 r.).

<sup>19</sup> C.M. Bast-Ransford, C. Pyle, Legal Research in the Computer Age: A Paradigm Shift?, *Law Library Journal* 2001, Nr 2, s. 285–302.

<sup>20</sup> Zob. https://www.lexisnexis.com.

<sup>21</sup> Zob. https://www.lexisnexis.com/en-us/products/lexis.page.

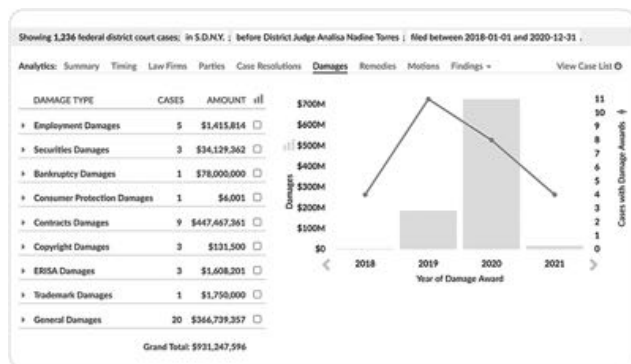
<sup>22</sup> Zob. https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-launches-lexis-answers-infusing-new-artificial-intelligence-capabilities-into-the-company-s-flagship-legal-research-platform-lexis-advance.

<sup>23</sup> Zob. https://www.alexsei.com/solution/#structure.

- b) odpowiedzi, która zawiera ważniejsze przepisy prawne, zasady prawa i ewentualne wcześniejsze orzeczenia sądowe;
- c) dodatkowych informacji prawniczych, które dotyczą głównie praktyki dotkniętego pytaniem organu państwowego (głównie sądu) lub innego.

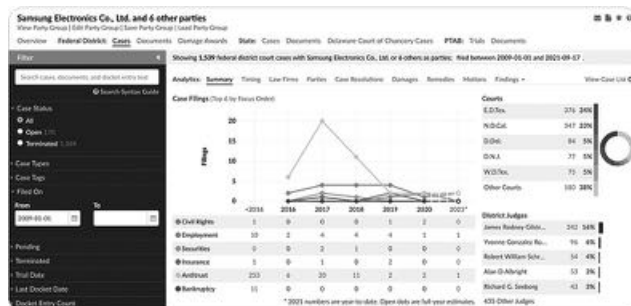
### 1.3. Profilowanie sędziego prowadzącego sprawę i strony przeciwnej

Kolejną usługą LexisNexis jest aplikacja o trafnej nazwie Lex Machina<sup>24</sup>. Służy ona do analizy prawnej i oferuje nawet takie funkcje, jak – zakazane we Francji – profilowanie sędziego. Pozwala ona wyszukać np. wysokość odszkodowań zasądzonych w konkretnym okresie na danym obszarze przez konkretnego sędziego. Stosując metody statystyczne, program przewiduje również, jakie są szanse, żeby dany sędzia pozytywnie rozpatrzył dany wniosek, jak też daje odpowiedź na pytanie, w jakim czasie od wniesienia roszczenia można oczekiwać prawomocnej decyzji sądowej.



Rysunek 1: Fragment profilu sędziego wykonanego przez Lex Machina<sup>25</sup>

Lex Machina może być również wykorzystywana do profilowania strony przeciwnej lub jej pełnomocnika: jakiego rodzaju sprawy mieli przed danym sędzią lub sądem i w jaki sposób były one prowadzone, a w przypadku pełnomocnika: kim byli jego klienci, ile podobnych spraw już reprezentował itd. Oczywiście podstawą tych analiz jest fakt, że w Stanach Zjednoczonych, inaczej niż na Węgrzech, wszystkie powyższe dane są jawne.



Rysunek 2: Fragment profilu strony przeciwnej wykonanego przez Lex Machina<sup>26</sup>

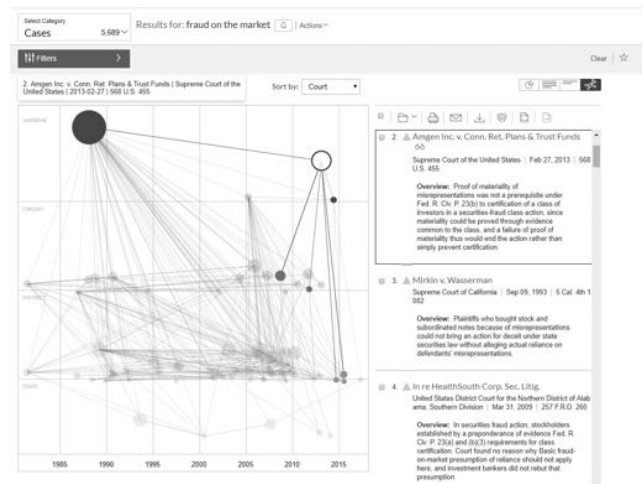
**Law Firms Report** Apple Inc. (Generated on 2023-09-16)  
Showing statistics for 1,406 cases from the Search for federal district court cases with Apple Inc. as a party, filed between 2009-01-01 and 2020-12-31. Limited to the top 1,000 law firms by total cases.

| Law Firm #                        | Total Cases # | Cases Representing the Selected Party Group # | Cases Opposed to the Selected Party Group # |
|-----------------------------------|---------------|-----------------------------------------------|---------------------------------------------|
| Nelson Bumgardner Albritton       | 132           | 55                                            | 71                                          |
| Ward, Smith & Hill                | 76            | 1                                             | 55                                          |
| McKool Smith                      | 71            | 0                                             | 52                                          |
| Prince Lobel Tye                  | 52            | 0                                             | 50                                          |
| Quinn Emanuel Urquhart & Sullivan | 93            | 3                                             | 49                                          |
| Russ August & Kabot               | 53            | 0                                             | 38                                          |
| Caldwell Cassidy & Curry          | 31            | 0                                             | 29                                          |
| Capshaw DeLineux                  | 48            | 0                                             | 27                                          |
| Hagens Berman Sobol Shapiro       | 33            | 1                                             | 22                                          |
| Susman Godfrey                    | 30            | 1                                             | 20                                          |

Rysunek 3: Fragment profilu strony przeciwnej wykonanego przez Lex Machina<sup>27</sup>

### 1.4. Wizualizacja orzecznictwa sądowego

Poza wykorzystaniem sztucznej inteligencji, LexisNexis kładzie duży nacisk na stosowanie technologii wizualizacji, które w branży prawniczej można uznać za stosunkowo słabo rozwinięte. Jednym z takich rozwiązań jest aplikacja Ravel View, która tworzy wykres 75 najlepiej trafionych orzeczeń sądowych i ich punktów stykających dla danego wyszukiwanego orzeczenia, pokazując poziomo datę wydania orzeczenia, pionowo instancję sądu wydającego orzeczenie (sąd miejski, sąd rejonowy, sąd okręgowy, sąd najwyższy), a kółkiem relewancję danego orzeczenia dla wyszukiwania (im większa, tym większa średnica):



Rysunek 4: Fragment wykresu wykonanego przez aplikację Ravel View<sup>28</sup>

<sup>24</sup> Zob. <https://lexmachina.com/legal-analytics/>.

<sup>25</sup> Źródło: <https://lexmachina.com/legal-analytics/>.

<sup>26</sup> Źródło: <https://lexmachina.com/legal-analytics/>.

<sup>27</sup> Źródło: <https://lexmachina.com/legal-analytics/>.

<sup>28</sup> Źródło: <https://www.lexisnexis.com/pdf/lexis-advance/Ravel-View-How-To-Literature.pdf>.

## 1.5. Westlaw

Angielski Westlaw<sup>29</sup>, podobnie jak LexisNexis, rozwinął się z mającej długą przeszłość prawniczej bazy danych w usługę, która wykorzystuje obecnie nowoczesne technologie do wspierania analizy orzecznictwa za pomocą sztucznej inteligencji. W istocie Westlaw oferuje dziś użytkownikowi dwa rozwiązania: aplikację Westlaw Classic, która zapewnia dostęp do aktów prawnych, orzeczeń, wzorów wniosków, a tym samym działa jako prawnicza baza danych w tradycyjnym rozumieniu tego słowa, oraz Westlaw Edge, która poza wyżej wymienionymi oferuje również analizę dokumentów i profilowanie oparte na sztucznej inteligencji.

## 1.6. AnyLaw

W platformie startowej AnyLaw<sup>30</sup>, opracowanej w Izraelu na bazie wyrafinowanych wyszukiwarek i uczenia maszynowego, punktem wyjścia było założenie, że dostęp do prawa (tj. ustaw, orzeczeń sądowych) powinien być szeroki, ponieważ są to informacje teoretycznie jawne dla wszystkich. Mimo to analiza orzecznictwa stanowi lwią część honorarium przedstawicieli prawnych, ponieważ niezbędne dane są dla laików trudno dostępne albo wręcz niedostępne. W przeciwieństwie do wymienionych wcześniej jest to usługa świadczona bezpłatnie, a polega głównie na przeszukiwaniu zebranej w niej bazy orzeczeń sądowych w Stanach Zjednoczonych.

# 2. Oprogramowanie wspierające pracę konkretnych organów wymiaru sprawiedliwości

## 2.1. Indie: SUPACE

Najważniejszym indyjskim oprogramowaniem wspierającym pracę sądów opartym na sztucznej inteligencji jest SUPACE, czyli *Supreme Court Portal for Assistance in Court Efficiency*. Jak wykazano wyżej, na obszarach anglosaskich najbardziej zainteresowany rozwojem oprogramowania jest sektor prywatny, natomiast w Indiach na czele wprowadzania innowacji stoi Sąd Najwyższy.

SUPACE, wprowadzony w 2019 r. na razie tylko w Bombaju i Delhi, o dziwo wyłącznie w postępowaniu karnym, opiera się w zasadzie na uczeniu maszynowym, a jego podstawę stanowią nagromadzone przez lata sprawy i wydane w nich orzeczenia sądowe. Sąd Najwyższy Indii nie chciał zapuszczać się na obszary bardziej drażliwe pod względem prawa do rzetelnego procesu sądowego, takich jak orzekanie, i wyraził się jasno, że jedynym celem SUPACE jest zmniejszenie obciążenia administracyjnego sądów i zaległości w sądach bez ingerowania w ich merytoryczną pracę<sup>31</sup>.

Jednym z głównych zadań SUPACE jest wybranie ze złożonych przez strony wniosków i dowodów faktów oraz danych istotnych dla sprawy, ażeby po takim „przesianiu” sędzia prowadzący mógł podjąć decyzję. Wszystko to S.A. Bobde<sup>32</sup>, który podczas wprowadzenia SUPACE był przewodniczącym Komisji Sztucznej Inteligencji Sądu Najwyższego, nazwał „postępowaniem hybrydowym”, ponieważ jego zdaniem sztuczna inteligencja najlepiej wykonuje swoją pracę wspólnie z inteligencją człowieka.

Zgodnie z dostępnymi obecnie informacjami nawał załatwionych spraw w sądach, w których wprowadzono SUPACE, zmniejszył się o około 20%<sup>33</sup>. Na tym jednak w Indiach nie poprzestano: rok później, w 2020 r., Sąd Najwyższy zakończył opracowywanie kolejnego oprogramowania, które w praktyce oznacza eliminację dokumentacji papierowej i zapewnia sędziemu prowadzącemu dostęp online do spraw.

## 2.2. Argentyna: Prometea

Ameryka Południowa, podobnie do północnej części kontynentu, pod względem zastosowania najnowszych technologii pojawiających się w dziedzinie wymiaru sprawiedliwości znajduje się w czołówce. Szczególnie interesująca jest Argentyna, która w październiku 2017 r. wprowadziła kompleksowy system o nazwie Prometea i od tego czasu aktywnie z niego korzysta. Ta aplikacja jest bardzo ważna również dlatego, że funkcjonuje w sądownictwie już stosunkowo długo – aż cztery lata, co w porównaniu z innymi przedstawionymi wyżej oprogramowaniami jest stosunkowo długim okresem (niektóre z nich wprowadzono tylko na próbę<sup>34</sup> lub działają od najwyżej rok lub dwa lata<sup>35</sup>).

Prometea została opracowana wspólnie przez Prokuraturę i Uniwersytet w Buenos Aires, które nie ukrywały, że ich celem było obniżenie obciążenia pracą i zwiększenie wydajności.

Główne funkcje programu Prometea można podsumować w czterech punktach:

a) działanie w charakterze inteligentnego asystenta;

<sup>29</sup> Zob. <https://legal.thomsonreuters.com/en/westlaw>.

<sup>30</sup> Zob. <https://www.anylaw.com/about>.

<sup>31</sup> S. Shekhar, Supreme Court embraces Artificial Intelligence, CJI Bobde says won't let AI spill over to decision-making, <https://www.indiatoday.in/india/story/supreme-court-india-sc-ai-artificial-intelligence-portal-supace-launch-1788098-2021-04-07> (dostęp z 1.1.2021 r.).

<sup>32</sup> G. Mishra, 'Judges' discretion retained' | SC's First AI-driven Research Portal 'SUPACE' Launched By CJI Bobde, <https://www.republicworld.com/india-news/general-news/scs-first-ai-driven-research-portal-supace-launched-by-cji-bobde.html> (dostęp z 1.1.2021 r.).

<sup>33</sup> T. Tandon, SUPACE Portal: Use of Artificial Intelligence (AI) in Indian Judiciary, <https://www.jagranjosh.com/general-knowledge/supace-portal-use-of-artificial-intelligence-ai-in-indian-judiciary-1618316032-1> (dostęp z 1.1.2021 r.).

<sup>34</sup> Np. Estonia.

<sup>35</sup> Np. Malesja: AISS oraz Indie: SUPACE.

- b) automatyczne generowanie dokumentów;
- c) samodzielne kategoryzowanie spraw
- d) i podobnie do prezentowanego poniżej programu COMPAS, przygotowywanie predykcji.

Mówiąc o inteligentnym asystencie systemu Prometea, najprościej jest porównać jego działanie do Siri – asystenta osobistego firmy Apple lub Alexa systemu Google. Analizuje (interpretuje) on bowiem pytanie w języku naturalnym jednocześnie z rozpoznawaniem mowy, następnie na nie odpowiada. Chociaż może to być przydatne, z pewnością nie jest to najważniejsza zaleta systemu.

Prawdziwą innowacją programu jest automatyczne generowanie dokumentu, w którym przetworzenie danych wejściowych następuje w ciągu kilku sekund (w zasadzie można sobie wyobrazić, że system „czyta”), a następnie program przygotowuje projekt orzeczenia.

Jeden z twórców Prometei – J.G. Corvolán, podał niezwykle imponujące dane w związku z tą funkcją: podczas gdy napisanie 1000 nakazów ochrony mienia za pomocą zasobów ludzkich zajmuje około 174 dni roboczych (prawie dziewięć miesięcy), Prometea pisze je w 45 dni. Wypisanie przez pracownika administracji prokuratora 1000 nakazów pracy zajmuje 83 dni robocze – Prometei zajmuje to tylko jeden tydzień roboczy, a więc pięć dni<sup>36</sup>.

To zaś, że w przypadku Prometei korektura literówek czy błędów rachunkowych jest zbędna, rozumie się prawie samo przez się. Wraz z wprowadzeniem aplikacji takie drobne błędy zostały praktycznie wyeliminowane.

Trzecia funkcja, czyli samodzielna kategoryzacja, ma również ogromne znaczenie, ponieważ potrafi ustalić priorytetową kolejność wszystkich wniosków i spraw w kilka sekund po przeanalizowaniu w krótkim czasie dużej ilości dokumentów. Wyobraźmy sobie, że program zdolny jest do filtrowania według słów kluczowych (np. „nieletni”, „dziecko”) i na tej podstawie ustalić, że dana sprawa musi być załatwiona w pierwszej kolejności, ponieważ dotyczy nieletniego. Do tej pory kategoryzacja również zajmowała długie dni – co samo w sobie stawia pod znakiem zapytania nadzwyczajną procedurę – a Prometea robi to w dwie minuty.

## Narzędzia proponujące treść wyroku

### 1. USA: COMPAS

Najbardziej znanym oprogramowaniem służącym do oferowania sędziom konkretnych propozycji orzeczeń jest COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) stosowany w kilku stanach USA (Nowym Jorku, Wisconsin, Kalifornii i na Florydzie) w celu podjęcia decyzji o ewentualnym zwolnieniu zatrzymanych.

Określone dane oskarżonego trzeba wprowadzić do systemu COMPAS niczym do formularza: toczące się przeciwko niemu postępowanie karne; wcześniejsze oskarżenia; przeszłość kryminalna; warunki mieszkaniowe; sytuacja rodzinna; używanie narkotyków; wiek; wykształcenie; zatrudnienie i źródła utrzymania. Naturalnie cały formularz jest znacznie bardziej szczegółowy: jak widać na przykładowej analizie ryzyka wykonanej przez COMPAS, system żąda podania 137 danych delikwenta.

Rysunek 5: Formularz danych do analizy ryzyka wykonywanej przez system COMPAS<sup>37</sup>

Odnosnie do danej osoby COMPAS potrafi wyliczyć trzy wskaźniki: ryzyko przedprocesowego zwolnienia; współczynnik recydywy i współczynnik recydywy o charakterze przemocowym<sup>38</sup>. Dane wprowadzone do systemu oceniane są przez COMPAS w skali od jednego do dziesięciu, a następnie sumowane i podawane w postaci współczynników końcowych, których wartości również zawierają się w przedziale od jednego do dziesięciu. Im wyższą wartość podaje COMPAS w wyniku swojej analizy, tym większe ryzyko niestawienia na rozprawie lub recydywy, a więc tym większą ostrożność musi zachować sąd przy zwolnieniu delikwenta.

COMPAS ostatecznie podaje trzy kryteria odnośnie do danej osoby, które nie są wiążące dla sądów, ale mogą stanowić dla nich pewne wskazówki w orzekaniu. Ważne jest jednak, że proces decyzyjny oparty na współczynnikach nie staje się automatyczny: sędzia w każdym przypadku musi rozważyć, w jakim stopniu weźmie pod uwagę wyniki obliczeń programu COMPAS, te bowiem, podobnie jak

<sup>36</sup> Zob. <https://www.thetechnolawgist.com/2019/06/20/entrevista-juan-gustavo-corvalan-buenos-aires-prometea-inteligencia-artificial/> (dostęp z 1.1.2021 r.). oraz <https://medium.com/astec/prometea-artificial-intelligence-in-the-judicial-system-of-argentina-4dfbde079c40> (dostęp z 1.1.2021 r.).

<sup>37</sup> Źródło: [https://s3.documentcloud.org/documents/2702103/Sample-Risk-Assessment-COMPAS-CORE.pdf?fbclid=IwAR1VIEP-M87ZnpbqAR9n1RNUmWNj\\_Ijxc7Fo77Hk\\_OCiXoRild\\_akvNTrA](https://s3.documentcloud.org/documents/2702103/Sample-Risk-Assessment-COMPAS-CORE.pdf?fbclid=IwAR1VIEP-M87ZnpbqAR9n1RNUmWNj_Ijxc7Fo77Hk_OCiXoRild_akvNTrA) (dostęp z 1.1.2021 r.).

<sup>38</sup> Practitioners' Guide to COMPAS Core. NORTHPOINTE, [http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-\\_031915.pdf](http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf) (dostęp z 1.1.2021 r.).

wszystkie wskaźniki oparte na zwykłych statystykach, są uproszczone i zniekształcające. Skutki te można wyeliminować, wprowadzając do kalkulacji wiele czynników, jednak, jak wskazał Sąd Najwyższy Wisconsin w lipcu 2016 r.<sup>39</sup>, wyniki, choć z prawnego punktu widzenia użyteczne, nadal mogą być dyskryminujące. Najczęstszym dylematem jest dyskryminacja rasowa: wiele uwzględnionych danych z konieczności dotyczy populacji afroamerykańskiej, która na ogół żyje w trudniejszych warunkach socjalnych. Złe warunki mieszkaniowe czy brak stabilnego zatrudnienia z pewnością zwiększą ryzyko recydywy, a wartości te będą mniej korzystne dla warstw biedniejszych, w których Afroamerykanie są nadreprezentowani.

Posiadający identyczną przeszłość kryminalną osoby czarnoskóre będą miały wyższy wskaźnik ryzyka niż inni oskarżeni, więc COMPAS w praktyce przyczyni się tylko do zaostrzenia i tak istniejących już dysproporcji społecznych i chociaż jego pierwotnym celem jest przewyższenie uprzedzeń, może łatwo stać się środkiem do ich pogłębiania<sup>40</sup>. Mimo to sąd prawdopodobnie postąpi słusznie, biorąc pod uwagę obliczenia takich systemów, potrafią one bowiem wykonywać tak skomplikowane analizy, do których sędzia-człowiek nie jest zdolny. Jednocześnie ważne jest, aby orzekanie na podstawie współczynników obliczanych przez sztuczną inteligencję nie stało się rutyną, choćby dlatego, że mechanizm działania COMPAS został utajniony przez jego twórcę, ponadto pojawiły się poważne wątpliwości co do wiarygodności jego predykcji<sup>41</sup>, sąd musi więc w każdym przypadku rozważyć, na ile realistyczne są wyniki obliczeń programu COMPAS. Współczynnik może być zatem przydatnym elementem podczas analizy ryzyka związanego z podsądnym, ale można na nim polegać jedynie jako na aspekcie bardziej złożonego procesu decyzyjnego<sup>42</sup>.

## 2. Meksyk: ExpertIUS

ExpertIUS to jedno z najstarszych oprogramowań opartych na sztucznej inteligencji z przeznaczeniem dla sądów, mamy jednak na jego temat niewiele informacji. Narzędzie to jest stosowane w sprawach z zakresu prawa rodzinnego, aby zdecydować, czy dana osoba powinna otrzymywać alimenty. Podczas rozstrzygania ExpertIUS opiera się na dostępnym mu orzecznictwie: identyfikuje wcześniejsze roszczenia alimentacyjne wysunięte w podobnej sytuacji i wydane w tych sprawach wyroki, a także bierze pod uwagę to, co zostało powiedziane na rozprawie<sup>43</sup>.

ExpertIUS nie jest w stanie ocenić kompleksowej sytuacji z zakresu prawa rodzinnego w całej jej złożoności, skupiając się wyraźnie na wycinkowej kwestii, czy strona jest uprawniona do świadczeń alimentacyjnych<sup>44</sup>.

The image shows a screenshot of the ExpertIUS software interface. At the top, it says 'CASO DE USO. (Ejemplo de navegación)'. Below that, there's a header with 'No. de Exp. XXX/2008', 'Pretensión: Fijación de Pensión Alimenticia', and 'Partes: Esposa vs. Esposo'. The main area has a horizontal navigation bar with buttons: 'FIJACIÓN DE LA LITIS', 'AUDIENCIA', 'EVALUACIÓN DE PRUEBAS', 'ALEGATOS', 'SENTENCIA', and 'DET. PENSION DEFINITIVA'. Below this, there's a list of tasks or steps: 'Admisión de la Demanda', 'Determinación de Pensión Provisional', 'Administración de la Contestación', and 'Ampliación de la litis'. To the right of this list, there's a button that says 'Determinar la procedencia de la suplencia de la queja'.

Rysunek 6: Formularz danych wymaganych do wykonania analizy programu ExpertIUS<sup>45</sup>

Ostateczny efekt jego analizy nie zamyka więc całej sprawy, a jedynie pomaga sądowi w kwestii alimentacyjnej, nie jest jednak dla niego wiążący. Ogólnie rzecz biorąc, w sprawach z zakresu prawa rodzinnego, w których rola czynnika ludzkiego jest szczególnie istotna, rozpowszechnienie sztucznej inteligencji napotyka naprawdę spore trudności.

## 3. Kolumbia: PretorIA

Trybunał Konstytucyjny Kolumbii otrzymuje co roku około 4000 wniosków o ubezwłasnowolnienie, a zajmuje się poważnie tylko ułamkiem z nich. Wcześniej zadaniem pracowników sądu było przetworzenie i przesianie tej ogromnej ilości podań oraz przedstawienie propozycji, które sprawy ma rozpatrywać Trybunał Konstytucyjny. Oprogramowanie o nazwie PretorIA zaoszczędza tego wielkiego nakładu pracy: we wnioskach o ubezwłasnowolnienie sztuczna inteligencja sprawdza obecność trzydziestu trzech kryteriów, potrafi nawet zestawić statystyki dotyczące występowania każdego z nich w orzecznictwie. Narzędzie interpretuje teksty wyroków i kategoryzuje je na podstawie wprowadzonych kryteriów, a także umożliwia szybkie wyszukiwanie

<sup>39</sup> State v. Loomis 881 N.W. 2d 749 (2016).

<sup>40</sup> J. Larson et alii: How we Analyzed the COMPAS Recidivism Algorithm, <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (dostęp z 1.1.2021 r.).

<sup>41</sup> E. Yong, A Popular Algorithm Is No Better at Predicting Crimes Than Random People, <https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/> (dostęp z 1.1.2021 r.).

<sup>42</sup> C.W. Johnson, The Increasing Risks of Risk Assessment: On the Rise of Artificial Intelligence and Non Determinism in Safety-Critical Systems, [http://www.dcs.gla.ac.uk/~johnson/papers/SCSC\\_18.pdf](http://www.dcs.gla.ac.uk/~johnson/papers/SCSC_18.pdf) (dostęp z 1.1.2021 r.).

<sup>43</sup> E. Cáceres, EXPERTIUS: A Mexican Judicial Decision-Support System in the Field of Family Law, Florence 2008, s. 54–57.

<sup>44</sup> Artificial intelligence and the judicial system in Latin America, World Today News, <https://www.world-today-news.com/artificial-intelligence-and-the-judicial-system-in-latin-america/> (dostęp z 1.1.2021 r.).

<sup>45</sup> Zródło: Conferencia Sistema EXPERTIUS: Sistema experto para la ayuda a la decisión judicial en la tradición romano-germánica, E.C. Nieto (IIJ-U-NAM). XIV Congreso Iberoamericano de Derecho e Informática, 26 octubre 2010, <https://www.youtube.com/watch?v=dJWwQztiLo> (dostęp z 1.1.2021 r.).

w orzecznictwie<sup>46</sup>. PretorIA potrafi opracowywać statystyki i sprawozdania z zakresu prawa precedensowego, ustalając, które przypadki mogą mieć największe znaczenie dla rozwoju orzecznictwa i wykrywania problemów systemowych<sup>47</sup>.

Rysunek 7: Wprowadzenie danych osobowych w celu otrzymania predykcji PretorIA<sup>48</sup>



Rysunek 8: Statystyka z wprowadzonych danych<sup>49</sup>

Tak więc PretorIA, podobnie jak badane do tej pory oprogramowanie, może być pomocna tylko w dobrze zdefiniowanym segmencie pracy sądowej, zastępując jednak znaczną część monotonnej, mechanicznej pracy człowieka i umożliwiając tym samym, żeby pracownicy sądowi skupili się na bardziej złożonych kwestiach prawnych<sup>50</sup>. Funkcjonowanie programu generalnie jest jednak kontrolowane przez ludzi: to oni określają kryteria oceny orzecznictwa dotyczącego ubezwłasnowolnienia, oni także wprowadzają tekst orzeczeń sądowych, wydanych w takich sprawach w Kolumbii. Sugestie programu PretorIA nie są wiążące dla Trybunału Konstytucyjnego, jednak ponieważ tu przetwarzanych jest tysiące spraw rocznie, w rzeczywistości więc prawdopodobieństwo dokonania przez człowieka merytorycznej rewizji jest przypuszczalnie mniejsze niż w przypadku obliczeń COMPAS lub ExpertIUS. PretorIA sygnalizuje jednak, że chociaż oprogramowanie oparte na sztucznej inteligencji nadal działa na podstawie statystycznych zestawień, jest w stanie wyjść poza obliczanie współczynników, a nawet może być zdolne do samodzielnego tworzenia treści tekstowych. Oczywiście, potraktowanie raportów PretorIA z należyтым dystansem leży już w gestii kolumbijskiego Trybunału Konstytucyjnego.

#### 4. Brazylia: Radar

O brazylijskim systemie Radar dostępnych jest niewiele informacji, podobnie jak w przypadku programu ExpertIUS, ale już na ich podstawie można wnioskować, że oprogramowanie stosowane w sądach brazylijskiego stanu Minas Gerais jest zbliżone do systemu PretorIA. Radar interpretuje pisma składane w sądzie i z użytych w nich pojęć wyciąga wnioski odnośnie do obowiązujących w stosunku do nich przepisów<sup>51</sup>. Ponadto narzędzie analizuje dotychczasowe orzecznictwo i przedstawia propozycję rozstrzygnięcia sprawy, która może być zrewidowana przez pracowników sądu lub sąd. Radar pracuje zatem z orzecznictwem dostarczonym przez ludzi, a dokumenty powstałe w wyniku jego analizy będą również w razie potrzeby zmienione przez człowieka.

#### 5. Malezja: Artificial Intelligence Sentencing System (AISS)

W ostatnim czasie zastosowanie sztucznej inteligencji eskaluje najszybciej chyba w malezyjskich sądach, chociaż ten kierunek rozwoju bynajmniej nie cieszył się powszechną aprobatą. Pierwsze kroki podjęto w tym kraju w pierwszych miesiącach 2019 r., kiedy przystąpiono do tworzenia oprogramowania do wykonywania pewnych segmentów pracy sądowej<sup>52</sup>. Pierwsze publiczne wystąpienie nowego narzędzia odbyło się w lutym 2020 r., wtedy jednak zamierzano jeszcze stosować je wyłącznie wobec zarzutów posiadania narkotyków lub przemocy seksualnej<sup>53</sup>. W lipcu 2021 r. ukazała się pierwsza instrukcja dla sądów dotycząca zastosowania nowej technologii, a jednocześnie rozpoczęto stopniowe poszerzanie jej zakresu. Nie jest jasne, na jakiej podstawie ustalono kolejność wprowadzania sztucznej inteligencji, w każdym razie po trzech fazach wdrożenia od kwietnia 2022 r. AISS będzie dostępny do kalkulowania sankcji dla wszystkich przestępców.

<sup>46</sup> F.A. Ogonjo, AI in the judicial system: possible uses and ethical considerations, <https://cipit.strathmore.edu/ai-in-the-judicial-system-possible-uses-and-ethical-considerations/> (dostęp z 1.1.2021 r.).

<sup>47</sup> The introduction of PretorIA, <https://ialab.com.ar/pretoria/> (dostęp z 1.1.2021 r.).

<sup>48</sup> Źródło: Laboratorio de Innovación e Inteligencia Artificial (IALAB): PretorIA: Inteligencia Artificial predictiva en la Corte Constitucional de Colombia, [https://www.youtube.com/watch?v=kq\\_N3r2diKw](https://www.youtube.com/watch?v=kq_N3r2diKw) (dostęp z 1.1.2021 r.).

<sup>49</sup> IALAB, i. m. (45. l.).

<sup>50</sup> J. Corvalan, The Study Case #1 – Use of Artificial Intelligence to Improve the Justice Service, <https://www.iltanet.org/blogs/juan-corvalan1/2021/05/06/the-study-case-1-use-of-artificial-intelligence-to> (dostęp z 1.1.2021 r.).

<sup>51</sup> Machine Learning & Big Data. Brazil. Global Legal Insights 2020, <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/brazil> (dostęp z 1.1.2021 r.).

<sup>52</sup> Malaysian judges to start using AI. 11.01.2019, <https://dig.watch/updates/malaysian-judges-start-using-ai> (dostęp z 1.1.2021 r.).

<sup>53</sup> O. Miwil, Malaysian judiciary makes history, uses AI in sentencing, <https://www.nst.com.my/news/nation/2020/02/567024/malaysian-judiciary-makes-history-uses-ai-sentencing> (dostęp z 1.1.2021 r.).

Zastosowanie AISS w żadnym wypadku nie jest obojętne, to do sądu należy decyzja, czy zasięgnąć opinii tego narzędzia. Zasada działania systemu polega na tym, że wypełniając coś na kształt formularza, należy wprowadzić odpowiednie dane oskarżonego (wiek, stan cywilny, przeszłość kryminalną, warunki mieszkaniowe), po czym na ekranie pojawia się sugerowana przez oprogramowanie kara, jak na przykład kara pozbawienia wolności na określony okres. Nawet jeśli sąd posłuży się sztuczną inteligencją, podana propozycja stanowi dla niego tylko pomoc, a *de facto* nawet po zapoznaniu się z sugerowaną karą, merytoryczna część procesu może być kontynuowana. Strony mogą zdecydować, czy zgodzić się na proponowany wymiar kary, czy też przedstawić argumenty za jej obojętnością lub obniżeniem.

Zwolennicy AISS twierdzą, że to nic innego jak tylko szybkie do uruchomienia narzędzie, które potrafi kalkulować wyroki w krótkim czasie i przeprowadzać osądy obiektywniej niż sędzia-człowiek. Ostatnie słowo i tak należy do sędziego, który ma prawo nawet całkowicie zignorować propozycję AISS, a ponieważ strony mogą zapoznać się z treścią wniosku jeszcze podczas rozprawy, mogą również wyrazić swoje poglądy na ten temat przed prawomocnym orzeczeniem sądu<sup>54</sup>.

Wiele osób uważa natomiast, że „nowa technologia, choć zapewnia sądom jedynie opcjonalne wsparcie, znacząco wypacza u sędziów tok myślenia, w dodatku czyni to całkowicie pomijając w swoich obliczeniach czynnik ludzki. Jednocześnie sztuczna inteligencja stanowi dla stron procesowych poważne źródło niepewności: już podczas pierwszego, próbnego zastosowania programu uczestnicy postępowania skarżyli się na zasięganie opinii u AISS, a spory z tym związane prowadzą do nieuzasadnionego przedłużania postępowania i utraty zaufania do sądu”<sup>55</sup>. Ponadto wcale nie jest jasne, co dzieje się między wprowadzeniem danych a wyświetleniem na ekranie proponowanej sankcji<sup>56</sup>.

W malezyjskiej dyskusji zwolennicy AISS wytoczyli jeszcze jeden argument, a mianowicie, że system opiera się na orzecznictwie człowieka, co oznacza obecnie orzeczenia sądów od 1.1.2014 r., a jego sugestie odnośnie kar również opierają się na praktyce sądowej z tamtego okresu<sup>57</sup>. Sztuczna inteligencja skutkuje zatem bardziej spójną praktyką sądową, co oznacza również dla stron większą przewidywalność. Zasadniczo zgadzając się z tym argumentem, autorzy niniejszego opracowania pragną dodać, że konieczne byłoby uważniejsze przeanalizowanie tego twierdzenia, gdyby baza danych AISS nadal opierała się głównie na orzeczeniach wydanych przez człowieka. Z czasem jednak decyzje podejmowane za pomocą sztucznej inteligencji mogą przeważać, co może rodzić ryzyko dalszego represjonowania w sądownictwie czynników ludzkich. Jednocześnie nie zapominajmy, że tak długo, jak ostatnie słowo należy do sędziego-człowieka, zasadniczo od nas zależy wykorzystanie korzyści płynących z tych nowych technologii i utrzymanie w ryzach ewentualnych wypaczeń.

Wszak na Węgrzech też istnieje alternatywna propozycja kary wnioskowana podczas procesu przez prokuraturę, która nie jest wiążąca dla sądu. Nie jest jasne, na podstawie jakich kryteriów wyznacza obecnie wysokość proponowanej sankcji węgierska prokuratura.

## 6. Chiny: sądy internetowe

Najbardziej bodajże popularnym przykładem sądów prowadzonych przez sztuczną inteligencję są Chiny. Pierwszy sąd internetowy powstał w 2017 r. w Hangzhou<sup>58</sup>, później zaś kolejno w Pekinie i Kantonie<sup>59</sup>. Takie postępowania sądowe można wszcząć w sprawach związanych ze światem Internetu (np. skargi dotyczące ochrony konsumentów, spory dotyczące praw autorskich w Internecie, płatności elektroniczne)<sup>60</sup>. W oparciu o aktualną wiedzę, chińskie sądy internetowe można zaliczyć właściwie do systemów wspierających orzeczenie sądu.

Ponadto chińskie sądy internetowe są w stanie przechowywać wprowadzone pisemnie lub zeskanowane przez strony dowody za pomocą technologii *blockchain*, aby można je było wykorzystać w procesie online. Jednocześnie jednak rozwiązanie to uniemożliwia przedstawianie sądowi innych treści niż te, które zostały wcześniej wgrane na platformę. Chińskie sądy internetowe identyfikują uczestników zgłaszających się na rozprawę online poprzez rozpoznawanie twarzy (*face recognition*), a program rozpoznawania mowy (*speech recognition*) pozwala na samodzielne wykonanie protokołu, czym system oszczędza pracownikom sądowym mnóstwo czasu i energii<sup>61</sup>. Oprogramowanie sądów internetowych potrafi również wyszukiwać orzecznictwo zgodnie z wprowadzonymi kryteriami i na tej podstawie kategoryzować wcześniejsze orzeczenia sądowe, podobnie do systemów PretorJA w Kolumbii, Prometheus w Argentynie czy Radar w Brazylii<sup>62</sup>.

<sup>54</sup> C.E. Ong, The AI Dilemma: Rise of the Machines in Malaysian Criminal Sentencing?, <https://legalatte.com/2021/07/26/the-ai-dilemma-rise-of-the-machines-in-malaysian-criminal-sentencing/> (dostęp z 1.1.2021 r.).

<sup>55</sup> V. Anbalagan, Malaysian Bar troubled over judges using AI for sentencing, [https://www.freemalaysiatoday.com/category/nation/2021/07/24/malaysian-bar-troubled-over-judges-using-ai-for-sentencing/?\\_\\_cf\\_chl\\_jschl\\_tk\\_\\_=zMqLEghlqOK0pE8vJ872tx.86zMw2JrTRmhlKa\\_4w-18-1636557255-0-gaNyGzNCyU](https://www.freemalaysiatoday.com/category/nation/2021/07/24/malaysian-bar-troubled-over-judges-using-ai-for-sentencing/?__cf_chl_jschl_tk__=zMqLEghlqOK0pE8vJ872tx.86zMw2JrTRmhlKa_4w-18-1636557255-0-gaNyGzNCyU) (dostęp z 24.2.2021 r.).

<sup>56</sup> Zob. więcej: Y. Bathae, The artificial intelligence black box and the failure of intent and causation, 31 Harvard Journal of Law & Technology 2018, s. 893–894.

<sup>57</sup> C.E. Ong, *op.cit.*

<sup>58</sup> Zob. oficjalną stronę internetową Sądu internetowego w Hangzhou: <https://www.netcourt.gov.cn/>.

<sup>59</sup> What's the magic of the Internet justice China program Cyberspace Administration of China, Legal Daily 2019, [http://www.cac.gov.cn/2019-12/12/c\\_1577686244875634.htm](http://www.cac.gov.cn/2019-12/12/c_1577686244875634.htm) (dostęp z 1.1.2021 r.).

<sup>60</sup> M. Zhu, Hangzhou Internet Court Pilot Application „AI Assistant Judge”, Hangzhou news 2019, [https://hznews.hangzhou.com.cn/jingji/content/2019-06/14/content\\_7210416.htm](https://hznews.hangzhou.com.cn/jingji/content/2019-06/14/content_7210416.htm) (dostęp z 1.1.2021 r.).

<sup>61</sup> G. Du, How the Beijing Internet Court Develops and Runs its IT System Inside China's Internet Courts Series 04, China Justice Observer 2019, <https://www.chinajusticeobserver.com/a/how-the-beijing-internet-court-develops-and-runs-its-it-system> (dostęp z 1.1.2021 r.).

<sup>62</sup> *Ibidem*.



Rysunek 9: Wideokonferencyjna rozprawa z prezentacją dowodów chronionych technologią blockchain<sup>63</sup>

Ponadto wiele chińskich sądów wykorzystuje oprogramowanie oparte na sztucznej inteligencji do automatyzacji pracy pracowników sądowych: chiński software potrafi rozpoznawać dostarczone dane i wstawić je do odpowiedniego formularza. W ten sposób sztuczna inteligencja może przygotować szereg akt sądowych, a nawet teksty wyroków i postanowień sądowych<sup>64</sup>. Usługa ta jest dostępna nie tylko dla sądu, ponieważ system może sporządzać wnioski również dla stron procesowych, jeśli otrzyma niezbędne do tego dane. Chińska technologia tym różni się od innych systemów wysuwających propozycje orzeczeń, że zastępujący pracę pracowników sądu tak naprawdę nie jest w stanie przedstawić konkretnej propozycji co do treści wyroku, ale jeśli zostaną jej dostarczone istotne elementy wyroku lub inny dokument procesowy, sformułuje dane akta, które oczywiście są następnie sprawdzane przez sędziów lub personel sądowy<sup>65</sup>. Podobną funkcją dysponuje argentyński system Prometea.

## Sztuczna inteligencja jako samodzielny decydent

### 1. Brazylia: VICTOR

Jako trzecią kategorię naszego badania przedstawimy stosowane już obecnie przykłady, w których decyzja sztucznej inteligencji całkowicie zastępuje wyrok sądu. W tym przypadku pominięto w procedurze akceptację człowieka, jest więc zrozumiałe, że do tej grupy należy najmniej podanych przez nas przykładów.

W Brazylii wprowadzono oprogramowanie sądowe o nazwie VICTOR<sup>66</sup> technologii rozpoznawania wzorców (*pattern recognition*). Brazylijskie najwyższe forum sądowe stosuje specjalny test dopuszczalności w celu oceny przedłożonych mu wniosków, biorąc pod uwagę wagę sprawy pod względem gospodarczym, politycznym i społecznym, decydując na tej podstawie o jego przydatności do oceny merytorycznej wniosku<sup>67</sup>. System VICTOR wykonuje ten test dopuszczalności bez interwencji człowieka<sup>68</sup>.

System wyciąga wnioski na podstawie predykcji dokonanej z tysięcy orzeczeń Sądu Najwyższego<sup>69</sup>. W tym sensie samo stworzenie bazy danych przedstawia istotne elementy dla administracji brazylijskiego sądownictwa, które po dokładnej analizie pozwalają na kwantyfikację poniższych zjawisk:

- a) najczęstszy rodzaj stron i spraw, które trafiają do Sądu Najwyższego;
- b) które kwestie kwalifikujące się na drogę sądową spełniają szczególny wymóg dopuszczalności;
- c) jakich kwestii konstytucyjnych dotyczą otrzymane wnioski i
- d) wyjątkowe przypadki powtarzających się i podobnych stanów faktycznych (które mogą stanowić precedens), ale nie pasują jeszcze do żadnego aktualnego tematu.

Po zsumowaniu tych danych możliwe jest dokładniejsze zbadanie dopuszczalności, co intensyfikuje systematyczny rozwój programu VICTOR<sup>70</sup>.

Chociaż pełna treść danej sprawy nie jest oceniana przez system VICTOR, to samodzielna decyzja o jej dopuszczalności przesądza o meritum sprawy, dlatego uważamy, że ze względu na konsekwencje również w tym przypadku sztuczną inteligencję należy uznać za decydenta, ponieważ jej decyzja wpływa też na meritum sprawy.

### 2. Argentyna: Prometea

W Argentynie prokuratura miasta Buenos Aires opracowała oprogramowanie o nazwie Prometea w celu przyspieszenia i automatyzacji postępowania sądowego, o czym już wcześniej mówiliśmy przy okazji innych kwestii. Jednak

<sup>63</sup> Źródło: CGTN: AI judges via chat app: the brave new world of China's digital courts, <https://www.youtube.com/watch?v=yuUN6VFWF-Q&t=14s> (dostęp z 1.1.2021 r.).

<sup>64</sup> G. Du, *op.cit.*

<sup>65</sup> S. Dai, Shanghai judicial courts start to replace clerks with AI assistants, South China Morning Post 2020, <https://www.scmp.com/tech/innovation/article/3077979/shanghai-judicial-courts-start-replace-clerks-ai-assistants> (dostęp z 1.1.2021 r.).

<sup>66</sup> Supremo Tribunal Federal de Brazil [Brazil Szövetségi Legfelső Bíróság]: Inteligência artificial vai agilizar a tramitação de processos no STF, JUSBRASIL 2018, <https://stf.jusbrasil.com.br/noticias/584499448/inteligencia-artificial-vai-agilizar-a-tramitacao-de-processos-no-stf> (dostęp z 1.1.2021 r.).

<sup>67</sup> M. Novello Siqueira, M. Castro, Brazil: The Supreme Federal Tribunal and the „General Repercussion „ Requirement, In: MONDAQ, 2008, <https://www.mondaq.com/brazil/constitutional-administrative-law/57864/the-supreme-federal-tribunal-and-the-general-repercussion-requirement> (dostęp z 1.1.2021 r.).

<sup>68</sup> N. Silva, F. Braz, T. de Campos, Document type classification for Brazil's supreme court using a Convolutional Neural Network, The Tenth International Conference on forensic computer science and cyber law, 2018, s. 7–11.

<sup>69</sup> V. Quezada, La inteligencia artificial transformará los procesos judiciales de Brasil, Techtarget 2018, <https://searchdatacenter.techtarget.com/es/cronica/La-inteligencia-artificial-transformara-los-procesos-judiciales-de-Brasil> (dostęp z 1.1.2021 r.).

<sup>70</sup> M. Filho, M. Said, T. Aguiar, Projeto VICTOR: Perspectivas de aplicação da inteligência artificial ao direito, Revista de Direitos e Garantias Fundamentais 2018, Nr 3, s. 219–238.

oprócz automatyzacji wykonywania dokumentów, Prometea potrafi również przygotowywać orzeczenia sądowych. Oprogramowanie działa jak chatbot, z którym każda strona może przedyskutować swoje kwestie prawne, gdy spór o pomoc społeczną trafi do sądu. Prometea potrzebuje sygnatury sprawy, aby odszukać dostępne już w tej sprawie dokumenty. Następnie bada sprawę poprzez dostęp online do ponad 300 000 orzeczeń sądowych. W przypadku odwołań dokonuje przeglądu akt sprawy, w tym wyroków sądów niższej instancji. Następnie czerpie wzorce z wydanych już w danej sprawie orzeczeń i porównuje je z wcześniejszymi opiniami prawnymi prokuratury<sup>71</sup>.



Rysunek 10: Działanie Prometei: komunikacja chatbota z klientem, następnie wyszukiwanie i prezentowanie akt sprawy<sup>72</sup>

Klientowi, który zwróci się do oprogramowania Prometea, na ekranie led pojawi się czat z małym logo, jak na przykład WhatsApp, następnie zaś klient może wybrać między procedurą telefoniczną a komputerową. Na wstępie procedury głos podobny do nawigacji GPS wita użytkownika i pyta „co będziemy dzisiaj robić?”. Po udzieleniu odpowiedzi program prosi klienta o numer pliku, a w dwie sekundy po odpowiedzi informuje, jaka jest okładka pliku i przedstawia rozwiązanie, które wydaje się najbardziej korzystne w tej sprawie. Trafność podejmowania decyzji algorytmicznych (umiejętność podejmowania takich samych decyzji w sprawach o identycznych faktach) została oceniona przez ekspertów na 94%<sup>73</sup>. Ponadto Prometea może być stosowana do monitorowania terminów i zasadniczych wymagań dotyczących wniosków sądowych oraz jako element pomocniczy w zamówieniach publicznych<sup>74</sup>.

### 3. Chiny i Estonia: mgliste informacje i plany

W związku z chińskimi sądami internetowymi z jednej strony pojawiły się artykuły prasowe, że strony mogą spotkać się na sali sądowej ze sztuczną inteligencją wyświetlaną jako hologram<sup>75</sup>, która w wyniku uczenia maszynowego podejmuje decyzję bez udziału człowieka<sup>76</sup>. Z drugiej strony istnieje wiele opinii czy reportaży<sup>77</sup>, które mówią o tym, że w sądach internetowych w rzeczywistości orzekają ludzie, a sztuczna inteligencja spełnia jedynie zadania administracyjne. Jak dotąd żadne stanowisko nie zostało bezspornie udowodnio-

ne, gdyż rzeczywistość Chin nie jest łatwa do spenetrowania. Dlatego też, ze względu na niepełne i sprzeczne informacje, ewentualnej funkcji samodzielnego orzekania oprogramowań opartych na sztucznej inteligencji w chińskich sądach internetowych nie analizujemy zbyt kompleksowo w niniejszym opracowaniu: dotykamy tego tematu tylko po to, aby objąć możliwie jak najszersze spektrum.

Idea algorytmicznego orzecznictwa przyciągnęła uwagę specjalistów pracujących nad usprawnieniem sądownictwa również w Europie: zmiany w estońskim systemie sądowym obejmują przekazywanie SI orzecznictwa w sprawach majątkowych do 7000 euro<sup>78</sup>. Inne inicjatywy estońskie mają na celu zastąpienie sędziów w zautomatyzowanych postępowaniach przyspieszonych odnośnie do nakazów zapłaty<sup>79</sup>. Projekty te są nadal na etapie przygotowawczym, jednak osiągnęły już na tyle zaawansowaną fazę, aby zwrócić uwagę, że inne (nawet europejskie) kraje mogą te rozwiązania docenić i wdrażać.

## Podsumowanie

Jak wspomniano na wstępie, w 2021 r., kiedy powstało to opracowanie, nie jest możliwe przedstawienie kraju i oprogramowania, gdzie – jak wyobrażają sobie laicy – za pulpitem sędziowskim faktycznie zasiada „sędzia-robot” i rozstrzyga spory. Orzecznictwo jako takie nie jest jeszcze obecnie – i chyba przez jakiś czas takie pozostanie – w pełni zautomatyzowane i nie ma bodaj takiej dziedziny prawa ani takiego kraju,

<sup>71</sup> E. Estevez, S. Linares Lejarraga, P. Fillottrani, Prometea Transformando la administración de justicia con herramientas de inteligencia artificial 2020, <https://publications.iadb.org/publications/spanish/document/PROMETEA-Transformando-la-administracion-de-justicia-con-herramientas-de-inteligencia-artificial.pdf> (dostęp z 1.1.2021 r.).

<sup>72</sup> Źródło: Prometea, <https://www.youtube.com/watch?v=yXEm8CL5HEg> (dostęp z 1.1.2021 r.).

<sup>73</sup> Zob. wywiad z J. Corvalánem, jednym z twórców Prometei, <https://www.ambito.com/politica/justicia/prometea-inteligencia-artificial-hacer-n5061091> (dostęp z 1.5.2022 r.).

<sup>74</sup> E. Murgo, Prometea, Inteligencia Artificial para agilizar la justicia 2019, <https://www.unidiversidad.com.ar/prometea-inteligencia-artificial-para-agilizar-la-justicia> (dostęp z 1.1.2021 r.).

<sup>75</sup> T. Vasdani, Robot justice: China's use of Internet courts, <https://www.lexisnexis.ca/en-ca/ihc/2020-02/robot-justice-chinas-use-of-internet-courts.page> (dostęp z 1.1.2021 r.).

<sup>76</sup> AI judges, verdicts via chat app: Brave new world of China's digital courts, Business Standard 2019, [https://www.business-standard.com/article/pti-stories/ai-judges-and-verdicts-via-chat-app-the-brave-new-world-of-china-s-digital-courts-119120600902\\_1.html](https://www.business-standard.com/article/pti-stories/ai-judges-and-verdicts-via-chat-app-the-brave-new-world-of-china-s-digital-courts-119120600902_1.html) (dostęp z 1.1.2021 r.).

<sup>77</sup> S. Soltan, Behind the headlines: Doubts about China's „robot judges”, Medium 2020, <https://medium.com/@sebastian.soltan/behind-the-headlines-doubts-about-chinas-robot-judges-20ce83862980> (dostęp z 1.1.2021 r.).

<sup>78</sup> P. Rabbitt, Estonia to Empower AI-based Judge in Small Claims Court, <https://150sec.com/estonia-to-empower-ai-based-judge-in-small-claims-court/10985/> (dostęp z 1.1.2021 r.).

<sup>79</sup> J.-M. Mandri, Kohtunikud saavad robotabilised: riik otsib võimalusi kohtusüsteemis tehisintellekti rakendamiseks, FORTE 2019, <https://forte.düelfi.ee/artikkel/85777829/kohtunikud-saavad-robotabilised-riik-otsib-voimalusi-kohtususteemis-tehisintellekti-rakendamiseks> (dostęp z 1.1.2021 r.).

w których sędziowie i pracownicy sądowi byłiby całkowicie zastąpieni przez oprogramowanie oparte na sztucznej inteligencji<sup>80</sup>. Nie należy zatem się tego spodziewać na Węgrzech czy w innych krajach regionu jeszcze przez długi czas.

Zanim dojdzie do rozpatrywania kwestii etycznych, filozoficznych i moralnych tego zagadnienia, warto przyrzeć się systemom wspomagania podejmowania orzeczeń i oferowania propozycji decyzji, na polu których dokonał się w ostatnich latach ogromny rozwój, a niektóre kraje takie technologie stosują już nawet w praktyce. Opracowując te programy, każdy kraj czy firma skupiły się na tym, jakie inne, głównie administracyjne, działania i elementy zadań, poza orzecznictwem, wykonywane przez sędziów, a tym bardziej pracowników wymiaru sprawiedliwości, można by skutecznie zastąpić lub wesprzeć systemem opartym na sztucznej inteligencji, tak aby nie dotykać kwestii praw człowieka, etyki i moralności.

Zbadanie tych tak zwanych oprogramowań wspierających jest konieczne tym bardziej dlatego, że można się spodziewać, że w niedalekiej przyszłości bezsprzecznie to one będą się najprędzej rozprzestrzeniać, właśnie dlatego że ich stosowanie nie powoduje problemów etycznych związanych z podstawowymi ramami postępowania sądowego i niekoniecznie pociąga za sobą poważne zmiany legislacyjne, a korzyści z ich wprowadzenia są niezaprzeczalne. Taką korzyścią

jest na przykład skoncentrowanie ludzkiej siły roboczej na ważniejszych zadaniach: sędzia będzie miał więcej czasu na zajęcie się merytorycznymi sprawami, jeśli SI wcześniej przeanalizuje złożone wnioski i wykona dla niego wyciąg istotnych dla sprawy danych, ewentualnie przeprowadzi zamiast niego analizę orzecznictwa, co on będzie musiał tylko sprawdzić. W związku z rozpowszechnianiem się tych technologii nadal jednak trzeba zwracać szczególną uwagę na aspekty gwarancyjne.

Jednocześnie nie można i nie wolno lekceważyć kwestii, czy możliwe jest zastąpienie orzecznictwa i ludzkich sędziów sztuczną inteligencją, twierdząc, że sztuczna inteligencja stwarza zbyt wiele zagrożeń prawnych i nie powinna być w ogóle dopuszczana do wymiaru sprawiedliwości. Potrzebna jest bezustanna, wielopłaszczyznowa debata, kwestionowanie i monitorowanie praktyk międzynarodowych, po to aby wstępując na coraz to nowe etapy czwartej rewolucji przemysłowej, zachować w Europie Środkowej wartości naszych systemów prawnych, przy jednoczesnym percypowaniu i modyfikowaniu tego, co już przestarzałe i nieskuteczne.

<sup>80</sup> Jak wyjaśniono w trzeciej części: nie mamy wystarczających informacji na temat Chin, aby kategorycznie to potwierdzić.

**Słowa kluczowe:** sztuczna inteligencja w zastosowaniu sądowym; innowacje sądowe; cyfryzacja sądów; zautomatyzowane podejmowanie decyzji; przełomowa technologia; sąd informatyzacji; AI; oprogramowanie oparte na sztucznej inteligencji; sąd online.

## Artificial Intelligence-based software in courts around the world: relevant practice, experience, and challenges for Hungary and Central-Europe

*In recent years, in the field of science there have been debates on the possibility of applying Artificial Intelligence in courts with participants from any discipline. And so it is in Hungary. However, adversarial views are stuck on the level of generalizations based on a theoretical square one, and legal science has not done a lot regarding the issue, mainly because of the lack of specific practical experience. In the present article, after the report on the current situation in Hungary, the authors will analyze which solutions are already in force abroad and what can be said about their effectiveness and influence on the procedures. The purpose is to put flesh on the modern technology, which is Artificial Intelligence-based software, to the readers, and active judges, representatives of legal professions, and also anyone who is currently looking for legal advice, or will do so in the future, or those who are interested in the future shape of courts. Such a seemingly distant process is not going to omit neither Hungary nor the whole region, therefore, it is crucial to address this modern branch of technology in courts.*

**Keywords:** AI in judicial application; court innovations; court digitization; automated decision-making; disruptive technology; court informatization; AI; AI-based software; online court.

Znajdź więcej nowości na:



ksiegarnia.beck.pl



## Elektroniczna licytacja nieruchomości

Krystyna Rogala<sup>1</sup>

Pandemia COVID-19 w sposób bezsprzeczny stanowiła impuls do dalszej informatyzacji postępowania cywilnego, w tym postępowania egzekucyjnego i upadłościowego. W okresie pandemii wprowadzone zostały zdalne rozprawy, uruchomiony został obligatoryjny e-KRS dla przedsiębiorców oraz Krajowy Rejestr Zadłużonych. Efektem tego kierunku legislacyjnego są również zmiany wprowadzone ustawą z 28.5.2021 r. o zmianie ustawy Kodeks postępowania cywilnego oraz niektórych innych ustaw<sup>2</sup>, jak doręczenia elektroniczne przez sądy dla profesjonalnych pełnomocników, a także, od lat postulowana przez doktrynę, regulacja elektronicznej egzekucji z nieruchomości. Niniejsze opracowanie ma na celu omówienie wprowadzonej instytucji elektronicznej egzekucji z nieruchomości na tle regulacji elektronicznych licytacji ruchomości oraz egzekucji z nieruchomości na zasadach ogólnych. Autorka analizuje również regulację systemu teleinformatycznego dla obsługi elektronicznych licytacji z nieruchomości jako systemu teleinformatycznego obsługującego postępowanie cywilne.

### Uwagi wstępne

Pandemia COVID-19 w sposób bezsprzeczny stanowiła impuls do dalszej informatyzacji postępowania cywilnego, w tym postępowania egzekucyjnego i upadłościowego. W okresie pandemii wprowadzone zostały zdalne rozprawy, elektroniczne doręczenia sądowe dla profesjonalnych pełnomocników, e-KRS czy Krajowy Rejestr Zadłużonych. Ruszyły elektroniczne licytacje ruchomości oraz nieruchomości. Choć wprowadzone instytucje nie pozostają bez wad, stanowią istotny krok dla polskiej legislacji w stronę dalszej informatyzacji.

Polski ustawodawca od dawna przejawia tendencje do wprowadzania przepisów prawnych przed dostosowaniem infrastruktury teleinformatycznej do ich pełnego zastosowania, co miało miejsce m.in. przy próbie uruchomienia tzw. Elektronicznego Biura Podawczego. Ustawą z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw<sup>3</sup> wprowadzono możliwość wyboru przez stronę postępowania wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego. Regulacja ta przewidywała, że w okresie trzech lat od wejścia w życie ustawy wnoszenie pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe będzie dopuszczalne, jeżeli ze względów technicznych leżących po stronie sądu będzie to możliwe. W tym czasie miał powstać system teleinformatyczny obsługujący tzw. Elektroniczne Biuro Podawcze. Po upływie trzech lat ustawodawca ustawą z 4.7.2019 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw<sup>3</sup> zmodyfikował brzmienie art. 125 KPC poprzez wprowadzenie § 2<sup>4</sup>, zgodnie z którym dokonanie wyboru wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego oraz dalsze wnoszenie tych pism za pośrednictwem tego systemu jest dopuszczalne, jeżeli z przyczyn technicznych, leżących po stronie sądu, jest to możliwe. Zmiana regulacji miała umożliwić dalszą pracę

nad systemem, który jednak, pomijając rozwiązania wyspowe, jak m.in. uruchomiony 1.12.2021 r. Krajowy Rejestr Zadłużonych, w dalszym ciągu nie powstał<sup>5</sup>.

Brak systemu teleinformatycznego stał się również przeszkodą dla pełnego uruchomienia elektronicznych licytacji ruchomości. Regulacja ta została wprowadzona ZmKPC15, jednak z uwagi na opóźnienia związane z tworzeniem systemu teleinformatycznego, pierwsze licytacje komornicze rozpoczęły się 1.3.2020 r. Opóźnienie związane było z brakiem środków finansowych na utworzenie i utrzymanie systemu teleinformatycznego przez Krajową Radę Komorniczą<sup>6</sup>.

Pandemia COVID-19 spowodowała, że potrzebne były doraźne, radykalne zmiany w funkcjonowaniu sądów, które pozwoliłyby zapewnić bezpieczeństwo stron postępowania i ich pełnomocników, sędziów oraz pracowników administracyjnych. Poprzez ZmKPC2021 dodano do ustawy z 2.3.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych<sup>7</sup> art. 15zszs. Na jego podstawie uruchomione zostały doręczenia dla profesjonalnych pełnomocników za pośrednictwem Portalu Informacyjnego. Doręczenie następuje poprzez umieszczenie ich treści w systemie teleinformatycznym. Datą doręczenia jest data zapoznania się przez odbiorcę z pismem lub

<sup>1</sup> Doktorantka w jednostce naukowo-badawczej Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) działającej w ramach Uniwersytetu Wrocławskiego. ORCID:0000-0001-6859-1474

<sup>2</sup> Dz.U. poz. 1090; dalej jako: ZmKPC2021.

<sup>3</sup> Dz.U. poz. 1311 ze zm., dalej jako: ZmKPC15.

<sup>4</sup> Dz.U. poz. 1469 ze zm.

<sup>5</sup> J. Gołaczyński, M. Dymitruk, Rozprawa zdalna i doręczenia elektroniczne w dobie pandemii COVID-19 po wejściu w życie nowelizacji z 28.5.2021 r., MoP 2021, Nr 13, s. 685.

<sup>6</sup> M. Domagański, Komornicze licytacje przez Internet nie ruszą od 1 marca, <https://www.rp.pl/zawody-prawnicze/art10613321-komornicze-licytacje-przez-internet-nie-rusza-od-1-marca> (dostęp z 20.12.2021 r.).

<sup>7</sup> T.j. Dz.U. z 2021 r. poz. 2095 ze zm.; dalej jako: tarcza antykryzysowa 3.0.

w przypadku braku zapoznania się z pismem, pismo uznaje się za doręczone po upływie 14 dni od dnia umieszczenia pisma w Portalu Informacyjnym. Doręczenie nie ma zastosowania do pism, które podlegają doręczeniu wraz z odpisami pism procesowych lub innymi dokumentami pochodzącymi spoza sądu. Przewodniczący może również odstąpić od doręczenia przez Portal Informacyjny, jeżeli jest to niemożliwe ze względu na charakter pisma. W praktyce pisma do listopada 2021 r. były umieszczane w zakładce „Dokumenty”. Pobranie dokumentu tam umieszczonego równoznaczne było z zapoznaniem się z pismem. W listopadzie 2021 r. uruchomiono nową funkcjonalność Portalu Informacyjnego poprzez dodanie zakładki „Moje doręczenia”, która dedykowana jest jedynie do doręczania pism procesowych w trybie art. 15zzs<sup>8</sup>. Doręczenie pisma za pośrednictwem Portalu Informacyjnego wywołuje skutki procesowe określone w Kodeksie postępowania cywilnego właściwe dla doręczenia pisma sądowego.

Tą samą ustawą do KPC został dodany (w części trzeciej, w tytule II w dziale VI po rozdziale 6) rozdział 6a „Sprzedaż nieruchomości w drodze licytacji elektronicznej”. Zgodnie z art. 7 pkt 1 ZmKPC2021 wejście w życie przepisów dotyczących licytacji elektronicznej nieruchomości zostało wydłużone trzymiesięcznym *vacatio legis* od dnia ogłoszenia aktu, tj. do 19.9.2021 r. Zgodnie z uzasadnieniem rządowego projektu wysiłki podejmowane w celu dalszej informatyzacji usług publicznych są uwarunkowane zaistniałą sytuacją epidemiologiczną i jej trudnym do przewidzenia zakończeniem<sup>9</sup>. Ustawa przewiduje, że w terminie roku od dnia jej wejścia w życie składanie wniosków o przeprowadzenie sprzedaży nieruchomości w drodze licytacji elektronicznej powinno być uzależnione od możliwości technicznych komornika.

Państwa członkowskie Unii Europejskiej w sposób odmienny regulują lub dotychczas nie podejmują próby stworzenia regulacji w przedmiocie licytacji elektronicznych. W 13 państwach członkowskich UE uruchomione zostały licytacje elektroniczne nieruchomości. Tyle samo państw umożliwia elektroniczną licytację nieruchomości. Zbiory tych państw nie są jednak tożsame. Tak na przykład Niderlandy, Litwa, Belgia pomimo uruchomienia licytacji online w zakresie nieruchomości nie regulują takiej możliwości w zakresie nieruchomości. Odwrotna sytuacja ma miejsce w Szwecji, Austrii i Niemczech, w których dopuszczalne jest prowadzenie elektronicznej egzekucji jedynie w zakresie nieruchomości.

Odmienne uregulowana została również kwestia przyznania kompetencji w zakresie uruchomienia i utrzymywania platformy czy platform, za pośrednictwem których prowadzone są licytacje, oraz charakter takich podmiotów. W Portugalii, Belgii, Estonii jest to organ samorządu zawodowego. W Niemczech, Austrii funkcję tę pełni organ rządowy. W Czechach, Finlandii rolę operatorów portali obsługujących sądowe egzekucje odgrywają prywatne podmioty<sup>10</sup>.

## Podstawowe zagadnienia

Podstawę regulacji elektronicznych licytacji nieruchomości stanowi KPC oraz wydane na podstawie delegacji ustawowej rozporządzenie Ministra Sprawiedliwości z 27.10.2021 r. w sprawie sposobu przeprowadzania sprzedaży nieruchomości w drodze licytacji elektronicznej oraz sposobu uwierzytelniania użytkowników systemu teleinformatycznego obsługującego licytację elektroniczną<sup>11</sup>. Licytacje elektroniczne obsługiwane są przez platformę E-LICYTACJE, utworzoną i utrzymywaną przez Krajową Radę Komorniczą<sup>12</sup>. Warunki określające sposób korzystania z Systemu E-licytacje zostały określone w Ogólnych warunkach użytkowania systemu e-licytacje<sup>13</sup>.

Gwoli wyjaśnienia wskazać należy, że w okresie od uruchomienia platformy od 1.3.2020 r. do 19.9.2021 r. były przeprowadzane elektroniczne egzekucje nieruchomości w trybie uproszczonej egzekucji nieruchomości, której przedmiotem

<sup>8</sup> G. Karaś, A. Zalesińska, [w:] J. Gołaczyński (red.), Postępowanie cywilne w czasie pandemii. E-doręczenia, rozprawa zdalna, posiadzenia niejawnie, składanie pism procesowych, Warszawa 2022, s. 70.

<sup>9</sup> Druk Nr 899 Rządowy projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw z 15.1.2021 r. – Uzasadnienie – <https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=899> (dostęp z 2.12.2021 r.).

<sup>10</sup> W Czechach brak jest jednej oficjalnej państwowej platformy aukcyjnej. Licytacje elektroniczne obsługiwane są przez wiele prywatnych portali, m.in. <http://www.exdrahy.cz> (prowadzony przez JURIS REAL), <http://www.okdrahy.cz> (prowadzony przez OK drahy s.r.o.), [www.e-aukce.com](http://www.e-aukce.com) (prowadzony przez NeutriCS a.s.) i inne – ([https://e-justice.europa.eu/473/EN/judicial\\_auctions?CZECH\\_REPUBLIC&member=1](https://e-justice.europa.eu/473/EN/judicial_auctions?CZECH_REPUBLIC&member=1)) (dostęp z 26.12.2021 r.).

<sup>11</sup> Dz.U. poz. 2005; dalej jako: rozporządzenie.

<sup>12</sup> Zob. <https://elicytacje.komornik.pl/> (dostęp z 11.12.2021 r.). Analiza regulacji elektronicznych licytacji nieruchomości w innych porządkach prawnych państw członkowskich Unii Europejskiej pozwala na wyszczególnienie następujących modeli legislacyjnych w ramach kryterium podmiotu odpowiedzialnego za utworzenie i utrzymanie systemu teleinformatycznego. Wśród grupy państw, które nie dopuszczają prowadzenia elektronicznych licytacji nieruchomości, wyróżnić można: 1) porządki prawne, w których uruchomiona została oficjalna platforma internetowa w celu publikacji obwieszczeń o prowadzonych licytacjach, 2) systemy prawne, które dopuszczają publikację obwieszczeń przez organy egzekucyjne na portalach komercyjnych. W ramach państw, które regulują przeprowadzanie elektronicznych licytacji nieruchomości, wyróżnić można: 1) porządki prawne, w których kompetencja do utworzenia i utrzymania platformy/platform, za pośrednictwem których przeprowadzane są licytacje nieruchomości, została powierzona podmiotom prywatnym, 2) w których kompetencja ta została powierzona podmiotom publicznym – organom samorządu zawodowego lub organom rządowym. Dokonując porównania powyższych rozwiązań z polską regulacją licytacji elektronicznych nieruchomości, wskazać należy, że wybrany przez polskiego ustawodawcę model regulacyjny w zakresie, w którym powierza on utworzenie i utrzymanie platformy organowi samorządu zawodowego – Krajowej Radzie Komorniczej odpowiada rozwiązaniom przyjętym m.in. na Węgrzech i w Portugalii. Nie jest to jednak dominujący model i funkcjonuje on równolegle do odmiennych rozwiązań – <https://arveres.mbvk.hu/reg.html> (dostęp z 24.12.2021 r.); <https://www.e-leiloes.pt> (dostęp z 26.12.2021 r.); <https://www.fina.hr/en/execution-of-enforcement-on-immovable-and-movable-property> (dostęp z 26.12.2021 r.); <https://e-justice.europa.eu> (dostęp z 26.12.2021 r.).

<sup>13</sup> Zob. <https://elicytacje.komornik.pl/rules> (dostęp z 20.12.2021 r.); dalej jako: Ogólne Warunki.

mogą być niezabudowane nieruchomości gruntowe oraz nieruchomości zabudowane budynkiem mieszkalnym lub użytkowym, jeżeli w chwili złożenia wniosku o wszczęcie egzekucji nie dokonano zawiadomienia o zakończeniu budowy albo nie wystąpiono z wnioskiem o udzielenie zezwolenia na użytkowanie w rozumieniu przepisów prawa budowlanego. Uproszczona egzekucja nieruchomości za pośrednictwem systemu teleinformatycznego prowadzona była na podstawie przepisów o licytacji ruchomości zgodnie z odwołaniem z art. 1013<sup>6</sup> § 1 KPC<sup>14</sup>.

Do sprzedaży nieruchomości w drodze licytacji elektronicznej zastosowanie ma regulacja dotycząca obwieszczenia licytacji, licytacji, warunków licytacyjnych, przybicia, z odrębnościami wynikającymi z regulacji sprzedaży nieruchomości w drodze licytacji elektronicznej. Licytacja elektroniczna przeprowadzana jest na wniosek choćby jednego wierzyciela. Taki wniosek może być również złożony w razie złożenia wniosku o wyznaczenie ponownej lub drugiej licytacji. W przypadku braku wskazania tejże formy odbycia przetargu przetarg będzie prowadzony zgodnie z ogólną regulacją<sup>15</sup>.

## Platforma e-licytacje jako system teleinformatyczny

Nowelizacją ZmKPC15 wprowadzono możliwość składania wniosków i oświadczeń za pośrednictwem systemu teleinformatycznego, gdy przepis szczególny tak stanowi lub dokonano takiego wyboru. Odpowiednikiem tejże regulacji w postępowaniu egzekucyjnym jest art. 760 § 1 KPC<sup>16</sup>, który stanowi *lex specialis* do art. 125 § 2<sup>1</sup> KPC. Wymóg wnoszenia pism za pośrednictwem systemu teleinformatycznego został uregulowany m.in. w zakresie elektronicznej licytacji ruchomości, w tym oświadczeń w trakcie, czy oświadczeń nabywcy o zrzeczenie się nabycia ruchomości (art. 879<sup>1</sup> i n. KPC), komunikacji między bankiem a komornikiem w przedmiocie zajęcia wierzytelności z rachunku bankowego (art. 893<sup>2a</sup> KPC) czy pism składanych przez organ podatkowy realizujący zajęcie wierzytelności z tytułu nadpłaty podatku albo zwrotu podatku (art. 902<sup>2</sup> § 3 KPC)<sup>17</sup>.

Wraz z wprowadzeniem regulacji dotyczącej elektronicznej licytacji nieruchomości katalog ten się poszerzył. Regulacja kodeksowa oraz rozporządzenie przewidują następujące wnioski i oświadczenia, które powinny zostać złożone za pośrednictwem systemu teleinformatycznego: wniosek o założenie konta użytkownika przez osobę posiadającą numer PESEL, zgłoszenie przystąpienia do przetargu, złożenie oświadczeń o braku podstaw do wyłączenia od udziału w nim, oświadczenia o działaniu w imieniu własnym lub cudzym, oświadczenia o pozostawaniu w związku małżeńskim oraz o zamiarze nabycia nieruchomości do majątku

wspólnego czy osobistego, uzupełnienie danych niezbędnych do przystąpienia na wezwanie komornika, dokonanie postąpienia, złożenie skargi na odmowę dopuszczenia do przetargu, na przebieg przetargu. Mając na uwadze brzmienie art. 760 § 1 zd. 2 KPC, uznać należy, że obligatoryjna elektroniczna forma wniosku i oświadczenia występuje tylko w przypadkach wprost wyrażonych w przepisach, a ich katalog jest zamknięty. Formę fakultatywną złożenia wybranych wniosków i oświadczeń za pośrednictwem systemu ogranicza natomiast jego funkcjonalność i brak technicznej możliwości złożenia danego pisma, niewymienionego wprost w przepisach, za pośrednictwem platformy. Przepisy art. 760 § 1 i 2 KPC odnoszą się do wszystkich systemów teleinformatycznych utworzonych w celu „obsługiwania” postępowań egzekucyjnych, należy mieć jednak na uwadze, że niektóre systemy teleinformatyczne, z uwagi na szczególne regulacje, nie dopuszczają złożenia oświadczenia o wyborze wnoszenia pism w formie elektronicznej, gdyż pisma muszą być wnoszone za pośrednictwem systemu<sup>18</sup>.

Podobnie wiele czynności egzekucyjnych podejmowanych przez komornika sądowego obligatoryjnie dokonywanych jest wyłącznie za pośrednictwem systemu teleinformatycznego – wyznaczenie licytacji, obwieszczenie o licytacji nieruchomości i udostępnienie protokołu opisu i oszacowania, wezwanie do uzupełniania danych niezbędnych do wydania postanowienia o przybicu, dopuszczenie licytanta do udziału w przetargu, informowanie o odmowie dopuszczenia do przetargu, zawiadomienie o wyłonieniu

<sup>14</sup> Tak m.in. I. Kunicki, [w:] A. Marciniak (red.), *Elektronizacja sądowego postępowania egzekucyjnego w Polsce*, Lex/el. 2015; A. Domoń, *Sprzedaż w drodze licytacji elektronicznej przez komornika sądowego po nowelizacji Kodeksu postępowania cywilnego dokonanej ustawą z 22 marca 2018 r. o komornikach sądowych*, PPE 2019, Nr 9, *passim*. Odmienne stanowisko zob. A. Pyrgies, *Sprzedaż nieruchomości w postępowaniu egzekucyjnym w formie licytacji elektronicznej*, PPE 2018, Nr 1 (suplement), *passim*.

<sup>15</sup> W analizowanych wybranych porządkach prawnych państw członkowskich UE – Czechy, Portugalia, Chorwacja, Węgry, większość państw (z wyjątkiem Węgier) dopuszcza prowadzenie za pośrednictwem systemu teleinformatycznego licytacji elektronicznej w ramach postępowania egzekucyjnego, postępowania upadłościowego i postępowania egzekucyjnego w administracji. Rozwiązanie takie należy ocenić pozytywnie, ponieważ pozwala na utworzenie jednego punktu dostępowego w Internecie, w ramach którego potencjalni nabywcy poszukiwać mogą informacji o prowadzonych licytacjach. Polskie rozwiązanie jest obecnie nastawione jedynie na egzekucję komorniczą w ramach postępowania cywilnego. Ewentualne otwarcie platformy na inne postępowania wymagałoby jego daleko idącej przebudowy i uelastycznienia – zob. <https://arveres.mbvk.hu/reg.html> (dostęp z 24.12.2021 r.); <https://www.e-leiloes.pt> (dostęp z 26.12.2021 r.); <https://www.fina.hr/en/enforcement-of-enforcement-on-immovable-and-movable-property> (dostęp z 26.12.2021 r.); <https://e-justice.europa.eu> (dostęp z 26.12.2021 r.).

<sup>16</sup> M. Uliasz, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Informatyzacja postępowania cywilnego. Teoria i praktyka*, Legalis/el. 2015; J. Studzińska, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Informatyzacja postępowania cywilnego. Teoria i praktyka*, Legalis/el. 2015.

<sup>17</sup> M. Uliasz, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Informatyzacja...*, Legalis/el. 2015.

<sup>18</sup> *Ibidem*.

licytanta oferującego najwyższą cenę czy anulowanie przetargu<sup>19</sup>. Doręczenia pism kierowanych przez komornika za pośrednictwem systemu teleinformatycznego są dokonywane obligatoryjnie w trybie opisanym w art. 131<sup>1</sup> KPC w zw. z art. 13 § 2 KPC<sup>20</sup>.

## Indywidualne konto w systemie teleinformatycznym

### 1. Rejestracja konta

Sprzedaż prowadzona jest za pośrednictwem systemu teleinformatycznego. W ramach systemu można wyróżnić funkcje: 1) dostępne bez konieczności uwierzytelniania, 2) dostępne jedynie dla osób uwierzytelnionych oraz 3) dostępne dla osób biorących udział w danej licytacji. Do pierwszej grupy zalicza się przeglądanie obwieszczeń umieszczonych na platformie. Następnie uwierzytelnienie umożliwia dostęp do protokołów opisu i oszacowania poszczególnych nieruchomości oraz wzięcie udziału w wybranej licytacji czy złożenie skargi na jej przebieg. Licytacja elektroniczna jest dostępna wyłącznie dla komornika oraz użytkowników biorących w niej udział<sup>21</sup>.

Rejestracja konta rozpoczyna się od złożenia wniosku w formie formularza zawierającego wiele danych takich jak: imię, nazwisko, numer PESEL, adres poczty elektronicznej, adres do korespondencji. Wnioskodawca oświadcza o prawdziwości wskazanych danych. Wniosek jest składany za pośrednictwem systemu teleinformatycznego. Imię, nazwisko oraz numer PESEL podlegają weryfikacji w rejestrze PESEL. W przypadku wykrytej niezgodności powiadamia się o odmowie założenia konta i poucza o możliwości złożenia wniosku za pośrednictwem wybranego komornika sądowego. Osoba chcąc założyć konto, a nieposiadająca numeru PESEL, może złożyć wniosek za pośrednictwem wybranego komornika sądowego. W takim wypadku wskazuje ona serię, numer i nazwę dokumentu potwierdzającego tożsamość oraz nazwę państwa, w którym wydano dokument. Komornik zakłada konto po przeprowadzeniu weryfikacji tożsamości wnioskodawcy. Kolejnych uwierzytelnień dokonuje się za pomocą loginu i hasła, gdzie login rozumiany jest jako niepowtarzalny i przyporządkowany do użytkownika zestaw danych wykorzystywanych przez niego do uwierzytelnienia w systemie teleinformatycznym<sup>22</sup>.

### 2. Indywidualne konto komornika

Korzystanie z platformy przez komornika sądowego lub asesora komorniczego działającego w zastępstwie komornika odbywa się po uprzednim zalogowaniu. Indywidualne konto komornika powiązane jest z uwierzytelnieniem w Systemie Komornik ID. Do logowania na platformie komornik

używa tych samych danych co do logowania do Systemu Komornik ID lub strony internetowej [www.komornik.pl](http://www.komornik.pl).

### 3. Konto dłużnika i wierzyciela

Na etapie rejestracji nie aktualizują się przesłanki z art. 976 KPC. Dopiero przy przystąpieniu do wybranego przetargu użytkownik zobowiązany jest do złożenia oświadczenia, iż nie zachodzą wobec niego podstawy do wyłączenia od udziału w przetargu, a więc czy nie jest on dłużnikiem, komornikiem, małżonkiem, dzieckiem, rodzicem i rodzeństwem dłużnika lub komornika. Nie istnieją jednak żadne przeszkody prawne, by dłużnik wyłączony od udziału w przetargu prowadzonym w postępowaniu egzekucyjnym wobec jego osoby brał równoległy udział w toczącym się na platformie innym przetargu.

W kontekście udziału uczestników egzekucji z nieruchomości pojawia się wątpliwość, czy platforma E-LICYTACJE pozwala na przejęcie na własność przez współwłaściciela nieruchomości wchodzącej w skład gospodarstwa rolnego (art. 958 KPC) oraz przejęcia na własność przez współwłaściciela, wierzyciela egzekwującego lub wierzyciela hipotecznego nieruchomości (art. 984 KPC). W pierwszej kolejności wskazać należy, że brak jest formalnych przeszkód dla rejestracji wierzyciela lub współwłaściciela na platformie E-LICYTACJE. Jednak ich udział w danej licytacji będzie uzależniony od przystąpienia do niej, wpłaty rękojmi i następczym dopuszczeniu przez Komornika do przetargu. Obecnie system teleinformatyczny przewiduje możliwość

<sup>19</sup> M. Uliasz, System teleinformatyczny obsługujący postępowanie egzekucyjne – analiza pojęcia, PPE 2017, Nr 4, *passim*; K. Flaga-Gieruszyńska, Pojęcie systemu teleinformatycznego w postępowaniu cywilnym, PPE 2017, Nr 2, *passim*. W zakresie aktualności definicji systemu teleinformatycznego zob. K. Flaga-Gieruszyńska, Elektroniczna doręczeń i zawiadomień w sądowym postępowaniu egzekucyjnym, PPE 2017, Nr 8, *passim*.

<sup>20</sup> K. Flaga-Gieruszyńska, Elektroniczna..., *passim*.

<sup>21</sup> Uprzednie uwierzytelnienie jest również wymogiem wzięcia udziału w licytacji elektronicznej w innych porządkach prawnych państwa członkowskich Unii Europejskiej (analizie w tym zakresie poddane zostały regulacje prawne w Czechach, Portugalii, Chorwacji i na Węgrzech). Proces uwierzytelnienia w systemie teleinformatycznym/systemach teleinformatycznych obsługujących licytacje elektroniczne nieruchomości w Czechach, Portugalii i na Węgrzech, podobnie jak w Polsce, został powiązany z procedurą tworzenia indywidualnego konta. W regulacji węgierskiej brak jest jednak możliwości uwierzytelnienia w ramach systemu, a dokonuje się jej w sposób stacjonarny poprzez okazanie dokumentu tożsamości wybranemu komornikowi sądowemu. W Chorwacji do uczestnictwa w wybranej licytacji nie jest konieczne posiadanie wcześniej założonego indywidualnego profilu na platformie. Potencjalny licytant, chcąc wziąć udział w licytacji, każdorazowo musi potwierdzić tożsamość ważnym cyfrowym certyfikatem lub przy użyciu certyfikatu umożliwiającemu użycie zaawansowanego podpisu elektronicznego. Następnie oferent wypełnia formularz rejestracyjny i podpisuje go podpisem elektronicznym zaawansowanym – zob. <https://arveres.mbvk.hu/reg.html> (dostęp z 24.12.2021 r.); <https://www.e-leiloes.pt> (dostęp z 26.12.2021 r.); <https://www.fina.hr/en/enforcement-of-enforcement-on-immovable-and-movable-property> (dostęp z 26.12.2021 r.); <https://e-justice.europa.eu> (dostęp z 26.12.2021 r.).

<sup>22</sup> A. Macuga, Sprzedaż ruchomości w drodze licytacji elektronicznej, DNCURRENDA 2017, Nr 1, *passim*.

złożenia zamkniętego katalogu wniosków i oświadczeń za jego pośrednictwem. Brak jest funkcjonalności dopuszczającej złożenie wniosku o przejęcie na własność nieruchomości, a tym samym skorzystania z dyspozycji art. 760 § 1 KPC poprzez dokonanie wyboru wniesienia pisma za pośrednictwem systemu teleinformatycznego.

#### **4. Przedstawiciel ustawowy, pełnomocnik, osoba uprawniona do działania w imieniu osoby prawnej albo innej jednostki organizacyjnej posiadającej zdolność prawną**

Odpowiednikiem § 9 rozporządzenia jest § 8 rozporządzenie Ministra Sprawiedliwości z 7.9.2016 r. w sprawie sposobu przeprowadzenia licytacji elektronicznej ruchomości w sądowym postępowaniu egzekucyjnym<sup>23</sup>, w którym została uregulowana kwestia korzystania z indywidualnego konta w systemie teleinformatycznym w cudzym imieniu<sup>24</sup>. Uprawniona osoba może wziąć udział w przetargu osobiście lub przez pełnomocnika. Zarówno działając w imieniu własnym, jak i jako pełnomocnik, przedstawiciel ustawowy albo osoba uprawniona do działania w imieniu osoby prawnej albo innej jednostki organizacyjnej posiadającej zdolność prawną, dany użytkownik korzysta z tego samego indywidualnego konta. By skutecznie działać w cudzym imieniu, konieczne jest spełnienie dwóch przesłanek. Po pierwsze, złożenie oświadczenia, o występowaniu w imieniu osoby trzeciej za pośrednictwem systemu teleinformatycznego, a po wtóre, załączenie utrwalonej w postaci elektronicznej kopii dokumentów potwierdzających uprawnienia do występowania w imieniu osoby trzeciej. Na gruncie regulacji elektronicznej licytacji elektronicznej pozostaje zatem aktualna kwestia niepołączalności ról. Pomimo braku limitu licytacji, w których dany użytkownik bierze udział, dany użytkownik nie może brać udziału w przetargu, w swoim imieniu oraz w cudzym równolegle. W dalszym ciągu dany licytant ma możliwość brania udziału w przetargu jako powiernik osoby trzeciej. W takim wypadku występować on będzie w przetargu w swoim własnym imieniu, a następnie po jego zakończeniu i prawomocnym przysądzeniu własności, przenieść własność nieruchomości na zleceniodawcę. Oświadczenie o roli w danym przetargu składane jest indywidualnie do każdego przetargu. Nie ma zatem możliwości jednorazowego określenia roli jako pełnomocnika, przedstawiciela ustawowego czy osoby reprezentującej<sup>25</sup>.

W doktrynie brak jest jednolitej definicji pełnomocnictwa procesowego. Przez niektórych autorów jest ono określane jako pełnomocnictwo do zastępowania strony lub uczestnika w postępowaniu sądowym<sup>26</sup> czy jako oświadczenie woli<sup>27</sup>, czy czynność prawna<sup>28</sup>, na podstawie której strona procesowa udziela osobie trzeciej upoważnienia do działania w sprawie cywilnej przed sądem w jego imieniu.

Ponadto jako pełnomocnictwo procesowe można rozumieć sam dokument zawierający takie oświadczenie<sup>29</sup>. Zgodnie z art. 91 KPC zakresem umocowania wynikającym *ex lege* z pełnomocnictwa procesowego są objęte wszelkie czynności dotyczące zabezpieczenia i egzekucji. Umocowanie to trwa – w braku odmiennego zastrzeżenia w jego treści – aż do prawomocnego zakończenia tych postępowań<sup>30</sup>. W przypadku gdy pełnomocnictwo zostało już przedłożone do akt sprawy sądowej, zbędne jest jego ponowne przedkładanie organowi egzekucyjnemu<sup>31</sup>. Obok pełnomocnictwa procesowego czynność procesowa może zostać dokonana na podstawie pełnomocnictwa do określonej czynności procesowej. Takim pełnomocnictwem jest uregulowane w art. 977 KPC pełnomocnictwo do udziału w przetargu. Konieczne jest zatem dokładne wskazanie określonej licytacji, do udziału w której pełnomocnictwo to umocowuje<sup>32</sup>. Regulacja ta przewiduje dwa wyjątki od norm ogólnych. Przede wszystkim art. 977 KPC nie ogranicza kręgu osób, którym można udzielić pełnomocnictwa do uczestnictwa w przetargu. Może być ono udzielone również podmiotom niewymienionym w art. 87 KPC<sup>33</sup>. Ponadto ustawodawca zdecydował się na modyfikację formy samego pełnomocnictwa, wprowadzając w tym zakresie bardziej rygorystyczny wymóg. Pełnomocnictwo do udziału w przetargu występuje w dwóch formach – dokumentu z podpisem urzędowo poświadczonym, w przypadku pełnomocnictwa udzielonego przez państwowe jednostki organizacyjne lub jednostki organizacyjne samorządu terytorialnego lub gdy umocowanym jest adwokat lub radca prawny – bez urzędowego poświadczenia podpisu.

Do pism, które z mocy przepisów szczególnych obligatoryjnie składane są za pośrednictwem systemu teleinformatycznego w ramach postępowania egzekucyjnego, odpowiednie zastosowanie będą miały niektóre przepisy

<sup>23</sup> Dz.U. poz. 1431.

<sup>24</sup> A. Domoń, Sprzedaż w drodze licytacji..., *passim*.

<sup>25</sup> I. Kunicki, Elektroniczna licytacja ruchomości w sądowym postępowaniu egzekucyjnym, *Lex/el.* 2019.

<sup>26</sup> J. Jodłowski, [w:] J. Jodłowski, Z. Resich, J. Lapierre i in., *Postępowanie cywilne*, Warszawa 2007, s. 245.

<sup>27</sup> K. Flaga-Gieruszyńska (red.), *Postępowanie cywilne. Komentarz praktyczny dla sędziów i pełnomocników procesowych*, *Legalis/el.* 2020.

<sup>28</sup> Tak: H. Mądrzak, [w:] H. Mądrzak (red.), *Postępowanie cywilne*, Warszawa, 2003, s. 120; A. Zieliński, *Postępowanie cywilne, Kompendium*, Warszawa 2004, s. 71.

<sup>29</sup> Tak m.in. J. Gudowski, *Pełnomocnictwo procesowe na tle podziału prawa na prywatne i publiczne*, *Polski Proces Cywilny* 2011, Nr 1, s. 7–27; tak też SN w wyroku z 22.10.2008 r., I UK 76/08, OSNP 2010, Nr 11–12, poz. 142; w postanowieniu SN z 10.7.2003 r., III CZP 54/03, *Biuletyn SN* 2003, Nr 7, s. 6.

<sup>30</sup> A. Olaś, komentarz do art. 91, [w:] P. Rylski (red.), *Kodeks postępowania cywilnego. Komentarz*, *Legalis/el.* 2021.

<sup>31</sup> I. Gil, komentarz do art. 91, [w:] E. Marszałkowska-Krześ (red.), *Kodeks postępowania cywilnego. Komentarz*, *Legalis/el.* 2021.

<sup>32</sup> P. Kuglarz, komentarz do art. 977, [w:] I. Heropolitańska (red.), *Komentarz do przepisów KPC regulujących egzekucję z nieruchomości*, *Legalis/el.* 2019.

<sup>33</sup> Zob. uchwałę SN z 23.7.2008 r., III CZP 56/08, OSN 2009, Nr 7–8, poz. 108.

o postępowaniu rozpoznawczym. W tym norma art. 68 § 2 KPC przewidująca zwolnienie przedstawiciela ustawowego, organ albo osoby wymienione w art. 67 KPC z obowiązku przedłożenia dokumentu wykazującego umocowanie w razie dokonania czynności procesowej za pośrednictwem systemu teleinformatycznego, w przypadku gdy przepis szczególny przewiduje, że czynności można dokonać wyłącznie za pośrednictwem tego systemu. Podmioty te zobligowane są jednak do wskazania podstawy swojego umocowania. Podobnie pełnomocnik procesowy, który wnosi pismo procesowe, w przypadku gdy przepis szczególny przewiduje, że czynności procesowej można dokonać wyłącznie za pośrednictwem systemu teleinformatycznego, nie ma obowiązku złożenia pełnomocnictwa, a jedynie powołuje się na nie, wskazując jego zakres oraz okoliczności wymienione w art. 87 KPC<sup>34</sup>. Regulacja § 9 rozporządzenia stanowi przepis szczególny względem regulacji ogólnej art. 89 § 1<sup>1</sup> KPC. Jednocześnie ustawodawca odmiennie niż w przypadku licytacji elektronicznej ruchomości reguluje wymóg złożenia dokumentu potwierdzającego uprawnienie do występowania w imieniu osoby trzeciej oraz łagodzi wymóg formalny art. 128 i 129 KPC. Ustawodawca w miejsce przedłożenia poświadczanego odpisu dokumentu wymaga bowiem złożenia jedynie utrwalonej w postaci elektronicznej kopii dokumentu potwierdzającego uprawnienie do występowania w imieniu osoby trzeciej. Regulacja ta nie wyłącza jednak zastosowania art. 977 KPC. Pełnomocnictwo, gdy udzielane będzie innym podmiotom niż profesjonalni pełnomocnicy i przez podmioty inne niż państwowe jednostki organizacyjne lub jednostki organizacyjne samorządu terytorialnego, winno być stwierdzone dokumentem z podpisem urzędowo poświadczonym. Dołączenie elektronicznej kopii tegoż dokumentu stanowić będzie przesłankę udziału jako pełnomocnik w licytacji elektronicznej nieruchomości. Analogicznie, w przypadku osób prawnych oraz jednostek organizacyjnych, które działają przez swoje organy albo przez osoby uprawnione do działania w ich imieniu, regulacja rozporządzenia stanowi *lex specialis* do norm art. 68 § 2 KPC. W toku licytacji elektronicznej nieruchomości umocowanie musi zostać wykazane kopią dokumentu potwierdzającego uprawnienie do występowania w imieniu osoby trzeciej.

## Obwieszczenie i złożenie rękojmi

Obwieszczenia o sprzedaży nieruchomości w drodze licytacji elektronicznej zamieszcza się na stronie internetowej Krajowej Rady Komorniczej co najmniej dwa tygodnie przed terminem licytacji. Zgodnie z art. 986<sup>4</sup> zd. 2 KPC do elektronicznych licytacji nie ma zastosowania obowiązek obwieszczenia w sądzie sprawującym nadzór nad egzekucją nieruchomości lub w lokalu organu gminy właściwym ze względu na miejsce położenia nieruchomości. Komornik nie

ma również uprawnienia do zawnioskowania o zarządzenie ogłoszenia w inny wskazany sposób, w szczególności w dzienniku poczytnym w danej miejscowości. Obwieszczenia o licytacjach nieruchomości są zatem publikowane wyłącznie na stronie Krajowej Rady Komorniczej oraz na platformie E-LICYTACJE<sup>35</sup>. Limit czasowy dokonania obwieszczenia pozostaje taki sam jak dla licytacji prowadzonej na zasadach ogólnych. Wraz z obwieszczeniem w systemie teleinformatycznym udostępniany jest protokół opisu i oszacowania nieruchomości<sup>36</sup>. To rozwiązanie koresponduje ze zmianą art. 953 § 1 pkt 5 KPC, wprowadzoną ZmKPC2021, którą zrezygnowano z udostępniania potencjalnym licytantom możliwości zapoznania się z całymi aktami postępowania egzekucyjnego i zastąpiono ją udostępnianiem jedynie protokołu opisu i oszacowania. Zgodnie z uzasadnieniem projektu rządowego poprzednie brzmienie przepisu umożliwiało „zbyt szeroki zakres pozyskiwania informacji o dłużniku przez osoby postronne”, co stało w sprzeczności z konstytucyjnymi gwarancjami ochrony prywatności i mogło prowadzić do stygmatyzacji, w szczególności w przypadku nieuprawnionego przetwarzania tychże informacji. Dostęp do całości akt postępowania był również zbędny z perspektywy nabywcy, dla którego wystarczająca, dla oceny przedmiotu licytacji winna być treść księgi wieczystej oraz protokół z opisu i oszacowania. Obwieszczenie o licytacji elektronicznej nieruchomości nie będzie również zawierało wskazania imienia i nazwiska dłużnika. „Niepożądane jest, aby w obwieszczeniu znajdowało się imię i nazwisko dłużnika. Wynika to z faktu, że dane osobowe umieszczone w Internecie bywają nierzadko powielane i mogłyby się one pojawiać w przestrzeni publicznej nawet wiele lat po zaspokojeniu wierzycieli. Taki stan rzeczy w sposób niedopuszczalny stygmatyzowałby dłużnika<sup>37</sup>”. W miejsce informacji o czasie i miejscu przeprowadzenia licytacji komornik powinien zawrzeć informację o tym, że przetarg odbywa się w drodze elektronicznej oraz o chwili jego rozpoczęcia i zakończenia. Komornik nie informuje również o możliwości złożenia rękojmi w formie książeczki oszczędnościowej zaopatrzonej w upoważnienie właściciela do wypłaty wkładu, z uwagi na wyłączenie tejże możliwości w stosunku do licytacji elektronicznej. Złożenie rękojmi następuje poprzez dokonanie wpłaty na rachunek bankowy

<sup>34</sup> M. Uliasz, [w:] J. Gołaczyński, D. Szostek (red.), Informatyzacja postępowania cywilnego. Komentarz, Legalis/el. 2016.

<sup>35</sup> Odmiennie przy elektronicznej licytacji ruchomości – A. Macuga, Sprzedaż ruchomości..., *passim*.

<sup>36</sup> Umieszczenie treści protokołu opisu i oszacowania w systemie teleinformatycznym było postulowane przy elektronicznych licytacjach ruchomości przez I. Kunicki, Elektroniczna licytacja w sądowym postępowaniu egzekucyjnym, [w:] A. Marciniak (red.), Elektroniczna sądowa egzekucja egzekucyjnego w Polsce, Sopot 2015, s. 262.

<sup>37</sup> Druk Nr 899 Rządowy projekt ustawy o zmianie ustawy- Kodeks postępowania cywilnego oraz niektórych innych ustaw z 15.1.2021 r. – Uzasadnienie, <https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=899> (dostęp z 2.12.2021 r.).

komornika, zamieszczany w treści obwieszczenia. Wpłata rękoi powinna zostać dokonana najpóźniej na dwa dni robocze przed rozpoczęciem przetargu. Ustawodawca zdecydował się zatem do skrócenia czasu na wpłatę rękoi, która zgodnie z art. 962 KPC przy egzekucji z nieruchomości na zasadach ogólnych może być wpłacona najpóźniej w dniu poprzedzającym przetarg. Do sprzedaży nieruchomości w drodze licytacji elektronicznej nie mają zastosowania zwolnienia od złożenia rękoi określone w art. 964 KPC dla osób, którym przysługuje ujawnione w opisie i oszacowania prawo, jeżeli jego wartość nie jest niższa od wysokości rękoi i jeżeli do tej wysokości znajduje ono pokrycie w cenie wywołania wraz z prawami stwierdzonymi w opisie i oszacowaniu, korzystającymi z pierwszeństwa przed jej prawem. Tym samym nie znajdzie zastosowania art. 969 § 2 KPC przewidujący, iż od nabywcy nieskładającego rękoi, który nie wykonał warunków licytacyjnych, ściąga się rękoi w trybie egzekucji należności sądowych. Odmienne przy elektronicznej licytacji nieruchomości złożenie rękoi może nastąpić alternatywnie za pośrednictwem systemu teleinformatycznego bądź (bezpośrednio) komornikowi. Złożenie rękoi za pośrednictwem systemu teleinformatycznego powoduje automatyczne przypisanie użytkownikowi unikalnego identyfikatora licytanta. Natomiast złożenie rękoi komornikowi powoduje konieczność następczego potwierdzenia jej złożenia w systemie teleinformatycznym i przypisania licytantowi unikalnego identyfikatora<sup>38</sup>. W przyszłości postulowane jest dopuszczenie złożenia rękoi przy elektronicznej licytacji nieruchomości za pośrednictwem systemu teleinformatycznego.

Wraz z wpłatą rękoi konieczne jest podanie niezbędnych danych: numeru PESEL, numeru dokumentu stwierdzającego tożsamość, oświadczenia, czy uczestnik pozostaje w związku małżeńskim, a jeżeli tak, czy nieruchomość zamierza nabyć do majątku wspólnego czy osobistego, a także innych danych, jeżeli potrzeba ich podania wynika z przepisów odrębnych ustaw. Uczestnik wskazuje również, czy licytuje we własnym imieniu, czy jako pełnomocnik innej osoby. Do oświadczenia załącza się utrwalone w postaci elektronicznej kopie dokumentów potwierdzających uprawnienie do występowania w imieniu osoby trzeciej. Komornik ma uprawnienie do wezwania licytanta do uzupełniania danych lub, jeżeli udział w przetargu wymaga zezwolenia organu władzy publicznej lub wykazania do wystąpienia w imieniu innej osoby, do przedłożenia utrwalonych w postaci elektronicznej kopii wymaganych dokumentów, pod rygorem niedopuszczenia do udziału w przetargu, w terminie 3 dni, nie później niż dzień przed terminem licytacji. Po weryfikacji wpływu rękoi oraz niezbędnych danych komornik dopuszcza licytanta do udziału w przetargu. O odmowie dopuszczenia zawiadamia się zainteresowanego za pośrednictwem systemu teleinformatycznego. Osoba, której nie dopuszczono do przetargu, może w terminie 3 dni złożyć skargę za pośrednictwem systemu

teleinformatycznego. Po pozytywnej weryfikacji użytkownika zyskuje on możliwość dokonywania postępień w toku przetargu.

## Ramy czasowe licytacji oraz przebieg licytacji

Przetarg rozpoczyna się i kończy z chwilą wskazaną w obwieszczeniu o licytacji nieruchomości i trwa 7 dni. Wydłużenie czasu jego trwania ma przyczynić się do zwiększenia liczby uczestników, a tym samym uzyskania wyższej ceny nabycia<sup>39</sup>. Przetarg powinien zostać wyznaczony w taki sposób, aby zarówno termin rozpoczęcia, jak i zakończenia przypadł między godz. 9:00 a 14:00 w dzień roboczy. Aktualne pozostają rozważania co do czasu trwania elektronicznych licytacji nieruchomości. Szczególne uregulowanie terminu zakończenia licytacji powoduje, że nie znajdzie zastosowania art. 111 § 1 KC, zgodnie z którym termin oznaczony w dniach kończy się z upływem ostatniego dnia<sup>40</sup>. Licytacja zakończy się bowiem o wyznaczonej godzinie.

W toku przetargu licytanci oferują cenę nabycia za pośrednictwem systemu teleinformatycznego. Każdorazowo dokonanie postąpienia wymaga uwierzytelniania się na koncie użytkownika, utworzenia oświadczenia o postąpieniu oraz zatwierdzenia oświadczenia o postąpieniu. Po utworzeniu postąpienia w aktach sprawy automatycznie umieszczane jest potwierdzenie dokonania postępowania oraz nadany numer porządkowy. Licytanci mogą zapoznać się w systemie z informacją o najwyższym aktualnym postąpieniu, unikalnym identyfikatorze licytanta, który go dokonał, oraz czasie, który pozostał do zakończenia licytacji. Jedynie komornik sądowy ma dostęp do danych osobowych licytanta przed zakończeniem licytacji. Przetarg wygrywa licytant, którego oferta była w chwili zakończenia przetargu najwyższa. Ustalenie wygranego licytanta następuje automatycznie. O wyborze najwyższej oferty licytanci są informowani za pośrednictwem systemu teleinformatycznego. Zastosowania nie znajduje natomiast art. 980 KPC wskazujący, iż po ustaniu postępień komornik, uprzedzając obecnych, że po trzecim obwieszczeniu dalsze postąpienia nie będą przyjęte, obwieści trzykrotnie ostatnio zaofiarowaną cenę, zamknie przetarg i wymieni licytanta, który zaofiarował najwyższą cenę. Zakończenie przetargu następuje bowiem automatycznie w chwili wskazanej w obwieszczeniu. Od dnia zakończenia przetargu biegnie termin na wniesienie skargi na przebieg licytacji.

<sup>38</sup> R. Kulski, Sprzedaż ruchomości w drodze licytacji elektronicznej w Polsce, DNCURRENDA 2018, Nr 1, *passim*.

<sup>39</sup> Druk Nr 899 Rządowy projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw z 15.1.2021 r. – Uzasadnienie, <https://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=899> (dostęp z 2.12.2021 r.).

<sup>40</sup> R. Kulski, Sprzedaż ruchomości..., *passim*.

Niezwłocznie po zamknięciu przetargu, nie później niż w terminie tygodnia, komornik przesyła sądowi protokół z przebiegu przetargu, wszystkie nierozpoznane skargi oraz dokumenty niezbędne do udzielenia przybicia. Z licytacji elektronicznej komornik nie będzie sporządzał protokołu „papierowego”. Za wystarczające uznać można wydrukowanie zapisu przebiegu licytacji elektronicznej utworzonego w systemie teleinformatycznym. Jeśli licytacja elektroniczna nie dojdzie do skutku z powodu niezaoferowania ceny wywołania, komornik powinien sporządzić protokół „tradycyjny”, w którym stwierdzi, że licytacja nie doszła do skutku<sup>41</sup>.

Sąd albo referendarz sądowy wydaje postanowienie co do przybicia na posiedzeniu niejawnym w terminie tygodnia od dnia otrzymania protokołu z przebiegu przetargu oraz dokumentów niezbędnych do udzielenia przybicia. Sąd może wstrzymać wydanie postanowienia co do udzielenia przybicia, jeżeli skargi lub zażalenia wniesione w toku postępowania egzekucyjnego nie są jeszcze prawomocnie rozstrzygnięte. Wysłuchania licytanta, który zaoferował najwyższą cenę, oraz uczestników przetargu dokonuje się jedynie wtedy, gdy jest to konieczne do wydania postanowienia co do przybicia. Postanowienie co do przybicia doręcza się licytantowi, który zaoferował najwyższą cenę.

## Ograniczenia w stosowaniu regulacji dotyczącej elektronicznej licytacji nieruchomości

Nowa regulacja dotycząca elektronicznych licytacji nieruchomości nie może być obecnie w pełni wykorzystywana, z uwagi na obowiązujące ograniczenia egzekucji z nieruchomości. Dodany ustawą z 14.5.2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2<sup>42</sup> art. 952<sup>1</sup> KPC w § 5 przewiduje bowiem zakaz przeprowadzania licytacji lokalu mieszkalnego lub nieruchomości gruntowej zabudowanej budynkiem mieszkalnym, które służą zaspokojeniu potrzeb mieszkaniowych dłużnika w czasie obowiązywania stanu zagrożenia epidemicznego lub stanu epidemii oraz 90 dni po jego zakończeniu.

## Podsumowanie

Wprowadzenie możliwości przeprowadzania licytacji elektronicznych z nieruchomości należy ocenić pozytywnie. W szczególności w perspektywie działającego już od marca 2020 r. systemu teleinformatycznego, który mógł zostać dostosowany do nowej regulacji w zakresie licytacji nieruchomości. Z dużą dozą pewności regulacja ta przyczyni się do zwiększenia grona zainteresowanych udziałem w licytacjach z nieruchomości, co ma szczególną wagę

w przypadku tzw. trudnych sprzedaży o mniejszym potencjale ekonomicznym. Zwiększenie grona potencjalnych oferentów prowadzić będzie natomiast do uzyskania wyższej ceny nabycia, a tym samym wyższego stopnia zaspokojenia wierzycieli.

Ponadto elektroniczna licytacja nieruchomości, z uwagi na m.in. rezygnację z przeprowadzania posiedzenia jawnego i wysłuchania uczestników licytacji, przyczyni się do przyspieszenia postępowania. Pełna rejestracja przebiegu licytacji w systemie teleinformatycznym prowadzi natomiast do zwiększenia jej transparentności. Elementem, który obecnie dalej może budzić zastrzeżenia, jest konieczność dokonania wpłaty ręką, nie za pośrednictwem samego systemu, lecz za pomocą przelewu bankowego na rachunek komornika sądowego, co rodzi konieczność późniejszego dopuszczenia uczestnika do przetargu i pozostawia pole na ewentualny błąd. Możliwość wpłaty za pośrednictwem systemu teleinformatycznego istnieje w przypadku licytacji z ruchomości. Płatność za pośrednictwem platformy pozwoliłaby na zautomatyzowanie także tej części licytacji. Przy przystąpieniu do wybranej licytacji na platformie odnaleźć można informacje, że wprowadzenie takiej funkcji jest planowane.

Nie można również pominąć ogromnego znaczenia licytacji elektronicznych z perspektywy trwającej pandemii COVID-19. Regulacja ta znacząco ogranicza bowiem bezpośredni kontakt oferentów, sądu, komornika, zachodzący jedynie przy ewentualnej wizji lokalnej nieruchomości oraz w przypadku podjęcia decyzji przez sąd, na podstawie art. 986<sup>10</sup> § 2 zd. 2 KPC, o wysłuchaniu licytanta, który zaoferował najwyższą cenę oraz uczestników przetargu.

W dużej mierze wyeliminowane zostało również niebezpieczeństwo zmów oferentów czy namawiania przez jednego z uczestników do rezygnacji z udziału w licytacji pozostałych uczestników w czasie posiedzenia jawnego. Oferenci nie mają bowiem dostępu do swoich danych, a jedynie indywidualnie nadanych im identyfikatorów.

System teleinformatyczny stworzony na potrzeby licytacji ruchomości i nieruchomości w postępowaniu egzekucyjnym jest kolejnym rozwiązaniem wyspowym, częściowym. Ustawodawca zaniechał stworzenia systemu teleinformatycznego obsługującego postępowanie cywilne, tzw. Elektronicznego Biura Podawczego, które pozwoliłoby na kompleksową zdalną obsługę postępowania cywilnego. Ten trwający od lat stan prawny powoduje mnożenie szczegółowych regulacji prawnych odrębnych systemów teleinformatycznych, które często modyfikują normy ogólne KPC. Przykładem takiej normy *lex specialis* jest omawiany § 9 rozporządzenia. Dalsze kontynuowanie tej praktyki legislacyjnej prowadzi

<sup>41</sup> R. Kulski, Sprzedaż ruchomości..., *passim*.

<sup>42</sup> Dz.U. poz. 875 ze zm.

będzie, w ocenie autora, do braku kompatybilności szeregu stworzonych systemów teleinformatycznych, co w przyszłości przyniesie trudności w korzystaniu z nich przez uczestników obrotu. Negatywnie należy również ocenić enumeratywne

udostępnianie w systemie teleinformatycznym funkcjonalności w zakresie poszczególnych pism procesowych, co *de facto* powoduje brak możliwości skorzystania z normy art. 125 § 2<sup>1a</sup> KPC.

**Słowa kluczowe:** informatyzacja postępowania cywilnego, elektroniczna licytacja nieruchomości, egzekucja z nieruchomości, platforma e-licytacje.

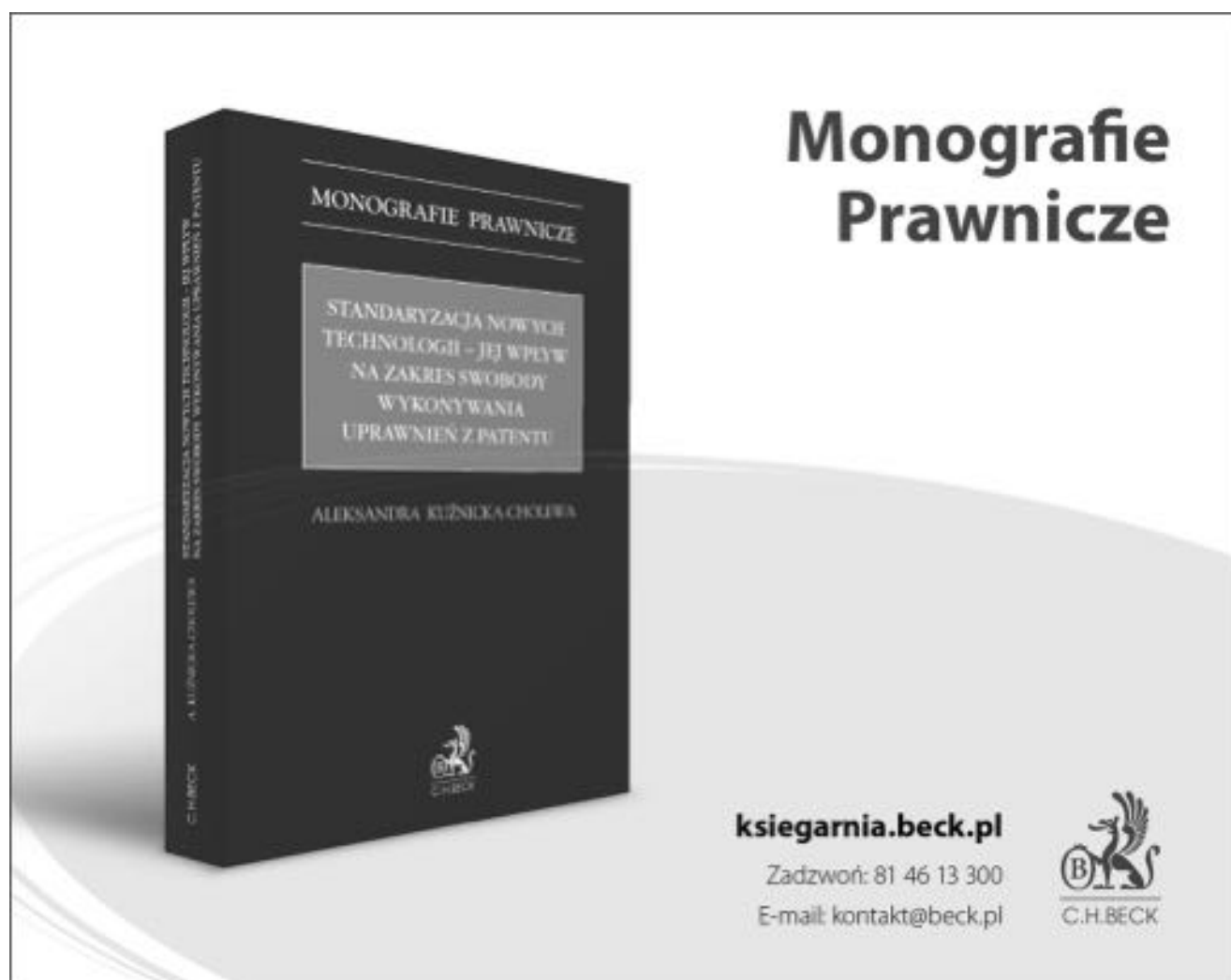
---

## Online judicial auction of real estate

*Undoubtedly, the COVID-19 pandemic was an impulse for further informatization of civil proceedings, including mortgage foreclosure and bankruptcy proceedings. During the pandemic remote court hearings were introduced. The obligatory e-KRS for entrepreneurs and the National Register of Debtors were launched. Other examples of this legislative direction were introduced by the Act of 28 May 2021 amending the Act – Code of Civil Procedure and certain other acts like courts' electronic service for professional attorneys, but also the regulation of the online judicial auction of real estate, long postulated by the doctrine. This study aims to discuss the introduced institution, also from the perspective of the regulation of electronic auctions of movable property and mortgage foreclosure according to general rules. The author also analyzes the regulation of the ICT system for electronic auctions of real estate as an ICT system supporting civil proceedings.*

**Keywords:** digitalization of civil proceedings, electronic auction of real estate, mortgage foreclosure, e-auction platform.

---



**Monografie  
Prawnicze**

**ksiegarnia.beck.pl**  
Zadzwoń: 81 46 13 300  
E-mail: kontakt@beck.pl

**C.H. BECK**

## LegalTech w kancelarii komorniczej

Klaudia Maciejewska<sup>1</sup>

Technologie transformacyjne służą cyfryzacji, digitalizacji, elektronizacji pracy komorników sądowych. Są sposobem na zwiększenie efektywności, produktywności, wydajności procesów prawnych. Nowoczesny komornik nie może funkcjonować bez wsparcia systemów informatycznych, teleinformatycznych czy też systemów eksperckich. Autorka przedstawia organizację pracy kancelarii komorniczych, możliwości, jakie niesie ze sobą *LegalTech*, możliwości zastosowania narzędzi informatycznych w pracy kancelarii komorniczych. Szczególną uwagę zwraca na bezpieczeństwo danych osobowych przetwarzanych w kancelariach komorniczych, stosowane środki bezpieczeństwa, a także zarządzanie bezpieczeństwem. Artykuł ma na celu wskazanie, że wdrażanie *LegalTech* w kancelariach komorniczych jest koniecznością. Stanowi wyzwanie związane ze zwiększonymi inwestycjami, reorganizacją modelu działania kancelarii, poszukiwaniem efektywności czasowej pracy czy też bezpieczeństwem przetwarzania danych osobowych oraz wymaga rozpoznania analizy ryzyka, rozliczalności, ochrony tajemnicy zawodowej.

### Uwagi wstępne

Nowe, innowacyjne technologie, w tym algorytmy i struktury wykorzystujące sztuczną inteligencję stanowią technologie transformacyjne. Stosowane w systemach informatycznych, teleinformatycznych służą cyfryzacji, digitalizacji, elektronizacji pracy komorników sądowych.

Komornicy sądowi i pracownicy kancelarii komorniczych stoją w obliczu ogromnych zmian w obszarach technologii, narzędzi i rozwiązań. *LegalTech* wpływa na organizację pracy kancelarii komorniczych, problematykę bezpiecznego gromadzenia danych osobowych w inteligentnych sieciach i systemach, przynosi nowe możliwości, korzyści.

Dostępne technologie, narzędzia i rozwiązania informatyczno-komputerowe służą zwiększaniu produktywności, wydajności, efektywności pracy kancelarii komorniczych, poprawie organizacji procesów w niej zachodzących, komunikacji elektronicznej, możliwości świadczenia pracy zdalnej. Zgodnie z uchwałą Rady Ministrów z 28.12.2000 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020”<sup>2</sup>, zmiana krajobrazu prawnego nastąpi w ciągu najbliższych trzech lat. *LegalTech* wpłynie na szersze zastosowanie technologii, zwiększenie inwestycji technologicznych, zwiększenie umiejętności i kompetencji informatycznych wśród pracowników kancelarii komorniczych, zrozumienie kierunku rozwoju i oczekiwań oraz zmianę przepisów prawa, która umożliwi szeroko pojętą cyfryzację i automatyzację postępowania egzekucyjnego, wykorzystywanie inteligentnych systemów bezpieczeństwa (ang. *smart security*), a także tworzenie i wdrażanie na rynek bezpiecznych systemów teleinformatycznych.

### Organizacja pracy kancelarii komorniczej

Zgodnie z art. 3 ust. 2 ustawy z 22.3.2018 r. o komornikach sądowych<sup>3</sup> czynności w postępowaniu egzekucyjnym i zabezpieczającym oraz inne ustawowe zadania komornik wykonuje osobiście. W przypadkach przewidzianych w ustawach komornik może zlecić wykonywanie określonych czynności asesorowi komorniczemu. Zlecenie wykonywania tych czynności jest dopuszczalne jedynie w celu przygotowania do wykonywania zawodu komornika. Przedmiotowa regulacja wprowadziła zasadę osobistego wykonywania czynności przez komornika i znacznie ograniczyła kompetencje pozostałych osób pracujących w kancelarii, jak aplikantów (art. 98 KomSądU), asesorów (art. 138 w zw. z art. 139 KomSądU), pozostałych pracowników kancelarii (art. 153 KomSądU).

W myśl art. 3 ust. 4 KomSądU komornikowi powierza się wykonywanie orzeczeń sądowych w sprawach o roszczenia pieniężne i niepieniężne oraz zabezpieczenie roszczeń, w tym europejskich nakazów zabezpieczenia na rachunku bankowym, z uwzględnieniem wyjątków przewidzianych w KPC, wykonywanie innych tytułów wykonawczych oraz tytułów egzekucyjnych, które podlegają wykonaniu w drodze egzekucji sądowej bez zaopatrywania ich w klauzulę wykonalności, wykonywanie postanowień o zabezpieczeniu środka dowodowego oraz postanowień nakazujących wydanie środka dowodowego w postępowaniu w sprawach własności

<sup>1</sup> Prawnik, doktorantka na Uniwersytecie Szczecińskim z programu Między Wydziałami Nauki i Szkolnictwa Wyższego „Doktorat wdrożeniowy”, inspektor ochrony danych, mediator sądowy, autorka publikacji z zakresu prawa nowych technologii, sądowego postępowania egzekucyjnego i ochrony danych osobowych. ORCID: 0000-0002-8498-841X.

<sup>2</sup> M.P. z 2021 r. poz. 23.

<sup>3</sup> T.j. Dz.U. z 2021 r. poz. 850 ze zm.; dalej: KomSądU.

intelektualnej, wykonywanie postanowień o zabezpieczeniu spadku lub sporządzanie spisu inwentarza, wykonywanie zadań określonych w innych ustawach. Komornik na zlecenie sądu albo wniosek powoda zobowiązany przez sąd na podstawie art. 139<sup>1</sup> § 1 KPC osobiście doręcza bezpośrednio adresatowi zawiadomienia sądowe, pisma procesowe oraz inne dokumenty sądowe za potwierdzeniem odbioru i oznaczeniem daty albo stwierdza, że adresat pod podanym adresem nie zamieszkuje, podejmuje czynności zmierzające do ustalenia aktualnego adresu zamieszkania adresata, sporządza protokół stanu faktycznego, a także na wniosek organizatora licytacji – sprawuje urzędowy nadzór nad dobrowolnymi publicznymi licytacjami, z przybicciem najniższej lub najwyższej oferty. Przedmiotowe czynności i zadania stanowią katalog zamknięty. Jednak, jak słusznie wskazuje K. Flaga-Gieruszyńska, nie ma znaczenia charakter czynności, która ma zostać wykonana, co oznacza, że obowiązek osobistego działania odnosi się do: czynności o charakterze zabiegów egzekucyjnych (np. doręczenie dłużnikowi nakazu wykonania aresztu – art. 1057 KPC); czynności badawczych (np. żądanie wyjaśnień niezbędnych do prowadzenia egzekucji – art. 761 KPC) oraz czynności decyzyjnych (np. postanowienia). W konsekwencji również w przypadku czynności o charakterze faktycznym odstępianie od osobistego wykonania ich przez komornika sądowego jest możliwe jedynie w przypadkach dopuszczonych *expressis verbis* w KomSądU<sup>4</sup>, do których należy w myśl art. 138 w zw. z art. 139 KomSądU katalog czynności, które komornik może zlecić do wykonania asesorowi komorniczemu w celu przygotowania do wykonywania zawodu komornika, na podstawie art. 98 KomSądU upoważnienie wydane przez komornika do podjęcia czynności przez aplikanta celem praktycznego przygotowania do wykonywania zawodu oraz zgodnie z art. 153 ust. 1a KomSądU upoważnienie wydane przez komornika do samodzielnego dokonywania czynności, o których mowa w art. 3 ust. 4 pkt 1 KomSądU przez pracownika kancelarii wydane po upływie sześciu miesięcy od dnia zawarcia umowy o pracę, przy czym pracownik nie może zostać skazany prawomocnym wyrokiem za przestępstwo lub przestępstwo skarbowe<sup>5</sup>.

Wprawdzie zasadą wprowadzoną KomSądU jest osobiste wykonywanie czynności przez komornika, jednak wiele zadań komornik realizuje przy pomocy kancelarii komorniczej, która ma charakter jednostki organizacyjnej indywidualnej, autonomicznej i służebnej wobec zadań powierzonych komornikowi sądowemu jako funkcjonariuszowi publicznemu.

Legalna definicja kancelarii komorniczej została uregulowana w art. 7 KomSądU. Zgodnie z jej brzmieniem komornik sądowy, w ramach pełnionej służby, organizuje indywidualną kancelarię komorniczą. Kancelaria to zespół osób i środków materialnych służących do obsługi komornika w zakresie powierzonych mu zadań i czynności. Siedziba kancelarii

znajduje się w rewirze komorniczym, w którym komornik został powołany. Komornik sądowy może prowadzić tylko jedną kancelarię. Komornik nie może tworzyć filii kancelarii, oddziałów ani innych jednostek organizacyjnych służących jej obsłudze.

Kancelaria komornicza stanowi jednostkę organizacyjną pracodawcy, w ramach której i za pomocą której komornik wykonuje swoje zadania<sup>6</sup>. Jest bowiem wyodrębniona organizacyjnie w zakresie m.in. lokalu, sprzętu biurowego, pracowników i prowadzona osobiście przez komornika<sup>7</sup>, a komornik sądowy dysponuje zapleczem osobowym, materialnym i organizacyjno-technicznym. Jak wskazał SN<sup>8</sup>, wykonywanie obowiązków komorniczych przy pomocy kancelarii jest obowiązkowe.

Zaplecze osobowe to zespół pracowników zatrudnionych w kancelarii komorniczej, który stanowi realne wsparcie w jej obsłudze, wykonywaniu czynności pomocniczych, takich jak przyjmowanie wpłat na kwitariusz, obsługa petentów, obsługa księgową, rejestracja spraw, podkładanie pism i zwrotnych potwierdzeń odbioru do akt spraw, przygotowywanie propozycji odpowiedzi na pisma, sporządzanie spisów zdawczo-odbiorczych, korespondencji do wysyłki, pomocy w czynnościach terenowych, archiwizacji akt spraw.

Do przedmiotowego zespołu pracowników zaliczyć należy kierownika kancelarii, aplikantów, asesorów komorniczych oraz pozostałych niezbędnych pracowników kancelarii, w tym pracowników biurowych, administracyjnych oraz podmioty niezbędne do ochrony mienia, z którymi komornik we własnym imieniu zawiera umowy o pracę, umowy o dzieło, umowy zlecenia lub umowy o świadczenie usług (art. 153 KomSądU), przy czym dla pracowników (w tym w szczególności asesorów i aplikantów komorniczych), z którymi komornik sądowy zawarł umowy o pracę, jest pracodawcą w rozumieniu art. 3 KP. Należy przy tym wskazać, że za działania osób zatrudnionych przez siebie, komornik ponosi odpowiedzialność odszkodowawczą jak za działania własne, a warunkiem koniecznym wystąpienia przedmiotowej odpowiedzialności jest powstanie szkody na skutek działania lub zaniechania działania osoby zatrudnionej przez komornika,

<sup>4</sup> K. Flaga-Gieruszyńska, Właściwość funkcyjna asesora i aplikanta komorniczego, [w:] A. Marciniak (red.), Analiza i ocena ustawy o komornikach sądowych oraz ustawy o kosztach komorniczych, Sopot 2018, s. 256.

<sup>5</sup> M. Uliasz, komentarz do art. 153, teza 2, [w:] J. Gołaczyński, D. Szostek (red.), Kodeks postępowania cywilnego. Komentarz do ustawy z 4.7.2019 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, wyd. 1, Legalis/el. 2020.

<sup>6</sup> K. Sadowski, komentarz do art. 8, teza 2, [w:] J. Świeczkowski, M. Świeczkowska-Wójcikowska, (red.), Ustaw o komornikach sądowych. Ustawa o kosztach komorniczych. Kodeks etyki zawodowej komornika sądowego. Komentarz, Warszawa 2020, s. 83.

<sup>7</sup> R. Reiwer, Komentarz do art. 7, teza 3, [w:] R. Reiwer (red.), Ustawa o komornikach sądowych. Ustawa o kosztach komorniczych. Komentarz, wyd. 1, Legalis/el. 2021.

<sup>8</sup> Zob. wyrok SN z 19.4.2010 r., II PK 298/09, Legalis.

przy czym działanie to lub zaniechanie musi pozostawać w związku z działalnością egzekucyjną<sup>9</sup>. Na komorniku spoczywa obowiązek kontrolowania czynności podejmowanych przez zatrudnione przez niego osoby. Brak przedmiotowej kontroli stanowi podstawę do poniesienia przez komornika odpowiedzialności dyscyplinarnej (art. 222 pkt 7 KomSądU).

Odnosząc się natomiast do środków materialnych wspierających komornika w zakresie wykonywania przez niego działalności egzekucyjnej i podejmowania czynności w myśl art. 3 KomSądU, składają się na nie m.in. aktywa trwałe w zakresie wyposażenia kancelarii komorniczej (sprzęt biurowy), urządzenia techniczne (zestawy komputerowe, nośniki danych), środki techniczne pomocne w gromadzeniu, selekcjonowaniu i przechowywaniu informacji (kserokopiarki, niszczarki, drukarki), środki transportu (samochody osobowe) oraz zasoby niematerialne, takie jak system informatyczny stanowiący wsparcie pracy kancelarii komorniczej, oprogramowania umożliwiające wykonywanie pracy zdalnej, usprawniające proces wystawiania faktur, system umożliwiający analizę orzecznictwa i doktryny, system aktów prawnych i publikacji. Środki materialne wykorzystywane są do realizacji określonych celów jak pozyskiwanie informacji prawnej, tworzenie dokumentów, rejestracja spraw i stanowią niezbędne narzędzia i realne wsparcie służące obsłudze kancelarii komorniczej.

Nie ulega wątpliwości, że zaplecze osobowe i środki materialne stanowią podstawę funkcjonowania kancelarii komorniczej, a na komorniku sądowym spoczywa obowiązek jej organizacji i utrzymania na poziomie odpowiednim do godności urzędu i posiadanych środków. Komornik obowiązany jest dbać o zachowanie kultury, najwyższy poziom profesjonalizmu swoich pracowników, w szczególności poprzez ich zaznajamianie w niezbędnym zakresie z obowiązującym stanem prawnym, oraz dbać, aby standard kancelarii odpowiadał pozycji organu władzy publicznej.

## Zastosowanie *LegalTech* w kancelarii komorniczej

Wyrażenie *Legal Technology* (technologie prawne; w skrócie *LegalTech*) pochodzi od połączenia słów „*legal service*” (obsługa prawna) oraz „*technology*” (technologie). W ustawodawstwie brak jest legalnej definicji *LegalTech*, natomiast w doktrynie technologie prawne określa się jako innowacje i rozwiązania technologiczne dedykowane prawnikom, a także narzędzia informatyczne, platformy i oprogramowania<sup>10</sup>. D. Szostek słusznie przedstawia podział *LegalTech* na trzy poziomy: 1.0, 2.0. oraz 3.0, gdzie *LegalTech* 1.0 odnosi się do technologii, w tym oprogramowania wspierającego działalność prawników jako profesjonalistów. Dotyczy to znanych od dawna systemów informatycznych do organizacji i funk-

cjonowania kancelarii prawnej, obiegu dokumentów, systemu informacji prawnej, systemów eksperckich, a także innych usług online, jak wideokonferencje, komunikacja online z sądami, rozprawy online, kształcenie online itd.

*LegalTech* 2.0 dotyczy znacznie bardziej zaawansowanej technologii, nie tylko wspierającej prawników, ale także zastępującej pracę ludzi – automatyzm czynności. Narzędzia *LegalTech* 2.0 są proponowane przez wielu dostawców, zarówno ze środowiska technologicznego, jak i ze środowiska prawnego czy naukowego. Wykorzystywane są w wielu czynnościach, jak ustalanie czy analiza faktów (m.in. stosowane przez organy śledcze), automatyczne tworzenie dokumentów, umów, pozwów itd. Do tej grupy narzędzi zaliczymy także *smart contracts* czy też tokenizację procesów.

Wreszcie *LegalTech* 3.0, w ramach którego wskazuje się nie tyle na automatyzm i zastępowanie człowieka przez technologię, ile na możliwość podejmowania autonomicznych decyzji. Wskazuje się tutaj na wykorzystanie AI lub zaawansowanych algorytmów wykorzystujących *machine learning*. *LegalTech* 2.0 to odtwarzanie wcześniej zaprogramowanych zdarzeń, automatyzacja, ale na wcześniej ustalonych zasadach. *LegalTech* 3.0 to wyższy poziom, gdzie decyzja podejmowana jest przez system na podstawie samodzielnie pozyskiwanych danych, samokształceniu się (które może przybierać różną formę). Ostateczna decyzja może być podejmowana bezpośrednio przez system informatyczny lub po jego akceptacji przez człowieka<sup>11</sup>.

Celem rozwiązań *LegalTech* w kancelarii komorniczej jest ułatwienie pracy z różnorakiego rodzaju przepisami i regulacjami, analiza orzecznictwa i doktryny prawnej, usprawnienie i zwiększenie wydajności procesów biurowych i organizacyjnych, automatyzacja prowadzenia czynności egzekucyjnych, tworzenie i zarządzanie dokumentami, rejestracja i monitorowanie czasu pracy, elektroniczne podpisywanie dokumentów.

Do najczęściej wykorzystywanych narzędzi informatycznych w pracy komornika sądowego należy zaliczyć kwalifikowany podpis elektroniczny (*E-signature*), narzędzia do organizacji pracy i komunikacji (*Workflow and Collaboration*), systemy informatyczne do zarządzania dokumentami oraz automatycznego ich gromadzenia (*Automatic Document Assembly*), E-BEL, E-CPD, system OGNIVO, Biuro

<sup>9</sup> A. Antkiewicz, komentarz do art. 153, [w:] G. Sikorski (red.), Ustawa o komornikach sądowych. Komentarz, Sopot 2019, s. 474.

<sup>10</sup> Blog Transparent Data, Co to jest LegalTech i jak można skategoryzować istniejące obecnie innowacje sektora prawnego, <https://medium.com/blog-transparent-data/co-to-jest-legaltech-i-dlaczego-co-raz-wi%C4%99cej-kancelarii-prawnych-si%C4%99ga-po-innowacje-2b2ff6b27ecd> (dostęp z 14.11.2021 r.).

<sup>11</sup> D. Szostek, Rozdział 1. Pojęcie Legal Technology (*LegalTech*), [w:] D. Szostek (red.), *LegalTech*. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym kancelarii oraz dziale prawnym, Legalis/el. 2021.

Informacji Kredytowej (BIK), ZUS-PUE, system Centralnej Ewidencji Pojazdów i Kierowców (CEPiK), aplikacja CEP, Elektroniczną Księgę Wieczystą (EKW), system Geoportal, Informator Prawno-Gospodarczy (IPG), baza REGON GUS, Centralną Ewidencję i Informację o Działalności Gospodarczej (CEDIG), Centralny Rejestr Podmiotów Krajowej Ewidencji Podatników (CRP KEP)<sup>12</sup>, a także systemy informatyczne służące wsparciu pracy kancelarii komorniczej, które zapewniają obsługę czynności merytorycznych postępowań oraz zarządzanie sprawami. Systemy informatyczne automatyzujące obsługę czynności biurowych i księgowych pozwalają komornikom przechowywać informacje o sprawach egzekucyjnych oraz prowadzić czynności dotyczące tych spraw dzięki kompleksowemu odzwierciedleniu procesów skoncentrowanych na ich merytorycznych aspektach. Przedmiotowe aplikacje systematyzują czynności postępowania egzekucyjnego, obsługują bezpieczne podpisy elektroniczne, współpracują z czytnikami kodów kreskowych, klientami poczty elektronicznej, a z zewnętrznymi systemami informatycznymi komunikują się za pomocą dokumentów w formacie XML oraz usług sieciowych. Natomiast wykorzystanie technologii OCR (ang. *Optical Character Recognition*) wraz z odpowiednimi skanerami dokumentów umożliwia wprowadzenie automatycznego przyporządkowywania korespondencji wpływającej do kancelarii komorniczej.

Komornicy sądowi przy wykonywaniu czynności i zadań nałożonych na nich przepisami prawa korzystają również z systemów informacji prawnej zawierających elektroniczne bazy danych złożone z dostępnych, opublikowanych aktów prawnych, orzecznictwa i baz danych jurysprudencji (poglądów doktryny zawartych w publikacjach monograficznych, komentarzach, czasopismach). Posługują się całokształtem legislacji zawartej na stronie internetowej Rządowego Centrum Legislacji, Dziennika Ustaw, Monitora Polskiego, Dziennika Urzędowego Unii Europejskiej oraz całokształtem orzecznictwa dostępnego na Portalu Orzeczeń Sądów Powszechnych, Bazie Orzeczeń Sądu Najwyższego, Internetowym Portalu Orzeczeń Trybunału Konstytucyjnego. Monitorują zmiany aktów prawnych, jednak przedmiotowe czynności odbywają się manualnie, bez wykorzystania narzędzi automatyzujących ten proces, ponieważ na rynku krajowym brak jest takiego narzędzia informatycznego. Podkreślenia przy tym wymaga, że realne usprawnienia czynności biurowych i organizacyjnych w kancelarii komorniczej, przy wykorzystaniu nowych, innowacyjnych technologii prawnych jest związane z wdrożeniem systemu teleinformatycznego z art. 158 KomSądU, w którym jest prowadzona i przechowywana dokumentacja w postaci akt elektronicznych (art. 155 ust. 1 KomSądU) i urządzenia ewidencyjne w formie elektronicznej (art. 156 KomSądU), integrującego się z innymi systemami teleinformatycznymi administracji publicznej, systemem teleinformatycznym obsługującym postępowanie sądowe, zabezpieczającego dane

osobowe przetwarzane w tym systemie oraz zapewniającego możliwość wymiany danych między użytkownikami systemu. System teleinformatyczny, stanowiąc realne wsparcie komorników sądowych, powinien dawać możliwość przechowywania i zabezpieczania akt spraw prowadzonych w postaci elektronicznej, możliwość prowadzenia urządzeń ewidencyjnych lub dokumentacji księgowej w postaci elektronicznej, umożliwiać identyfikację uczestników postępowań egzekucyjnych i zabezpieczających i ich pełnomocników oraz umożliwiać dostęp do systemu teleinformatycznego sądom, organom nadzoru administracyjnego oraz nadzoru wewnętrznego samorządu komorniczego. Należy przy tym podkreślić, że w systemie teleinformatycznym, zgodnie z art. 158 KomSądU, powinien zostać wdrożony moduł do prowadzenia elektronicznego biura podawczego, elektronicznej księgi nadawczej, umożliwiający obsługę doręczeń elektronicznych, sporządzanie elektronicznych protokołów, automatyzację procesu tworzenia pism, proponowania ich merytorycznej treści i podpowiadania kolejnych czynności w sprawie.

Zastosowanie *LegalTech* w kancelarii komorniczej związane jest również z cyfryzacją archiwizacji kancelarii komorniczych, która wiązałaby się z budową i wdrożeniem narzędzia wspomagającego zbieranie i klasyfikację zbiorów w postaci elektronicznej służących do uczenia z nadzorem. Przedmiotowe rozwiązanie związane jest z wprowadzeniem digitalizacji akt spraw komorniczych, tworzeniem cyfrowych repozytoriów, inteligentną analizą danych gromadzonych w procesie archiwizowania akt sprawy, tworzeniem konwersji dużej liczby dokumentów, a także automatyzacją procesów zachodzących w archiwizacji, w tym w procesie brakowania, udostępniania, niszczenia, przekazywania akt do Archiwum Państwowego.

Automatyzacja procesów przy wykorzystaniu nowych, innowacyjnych technologii, digitalizacja dokumentów, cyfryzacja i elektronizacja, wdrażanie *LegalTech* w kancelariach komorniczych wpływa na ich transformację, zwiększenie produktywności i wydajności zatrudnianej kadry, zmniejszenie wystąpienia błędów ludzkich. Umożliwia przetwarzanie większej ilości danych i spraw, zachowując ten sam poziom efektywności prowadzonych postępowań. Zastosowanie technologii prawnych wpływa również na skuteczniejsze zarządzanie, w tym na zarządzanie praktyką, radzenie sobie ze zwiększoną ilością i złożonością danych, lepsze świadczenie czynności.

Jak słusznie zauważa A. Klich, czynności egzekucyjne coraz częściej przybierają formę elektroniczną, co z całą pewnością pozytywnie wpływa na szybkość uzyskiwania niezbędnych informacji, czego wynikiem jest sprawniejsze

<sup>12</sup> K.R. Wisłocki, Informatyzacja postępowania egzekucyjnego z perspektywy komornika sądowego, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Informatyzacja postępowania cywilnego. Teoria i praktyka, Legalis/el. 2021.

przeprowadzenie postępowania egzekucyjnego. Zwiększona skuteczność komorników sądowych w zakresie pozyskiwania informacji może istotnie wpływać na podwyższenie efektywności całego postępowania egzekucyjnego. W pełni należy zaaprobować działania ustawodawcy zmierzające do rozwoju informatyzacji rejestrów i baz danych, poszerzając zakres prawa do informacji, które niewątpliwie przysługują wierzycielowi dochodzącemu swoich roszczeń w drodze przymusu, w ramach realizacji konstytucyjnie mu zagwarantowanego prawa do sądu<sup>13</sup>.

## Bezpieczeństwo danych osobowych w kancelarii komorniczej

Komornik sądowy, zgodnie z definicją zawartą w art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)<sup>14</sup> jest samodzielnym administratorem danych. Jak słusznie wskazuje *M. Jabłoński i K. Wygoda*, ostatecznie o tym, że komornicy traktowani są jako samodzielni administratorzy, świadczą rozwiązania zawarte w art. 158 ustawy z 21.2.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)<sup>15</sup>. Zasadniczo dotyczą one osób, których dane są przetwarzane (w następstwie skorzystania z dyspozycji zawartej w art. 23 RODO), ale stanowią potwierdzenie, że komornik sądowy traktowany jest jako administrator danych, na którym ciąży obowiązek sprecyzowane w RODO<sup>16</sup>.

Komornik sądowy jako administrator, wszczynając i prowadząc postępowanie, pozyskuje dane osobowe i przetwarza je za pomocą systemów, narzędzi *LegalTech*, stanowiących wsparcie tradycyjnej formy komunikowania się z organami i podmiotami zobowiązanymi do udzielania komornikowi sądowemu informacji niezbędnych do prowadzenia postępowania. Działalność kancelarii komorniczej to nie tylko akta komornicze, urządzenia ewidencyjne prowadzone przez komorników sądowych, ale także systemy informatyczne, teleinformatyczne. W myśl art. 159a KomSądU, administratorami danych znajdujących się w systemie teleinformatycznym, utworzonym do 1.1.2021 r., o którym mowa w art. 158 ust. 1 KomSądU, są komornicy w zakresie, w jakim dane te dotyczą prowadzonych przez nich spraw, a Minister Sprawiedliwości, jako administrator systemu teleinformatycznego, nie ma swobodnego dostępu do informacji w nim zawartych, w tym do danych osobowych.

Nie ulega przy tym wątpliwości, że dane osobowe zawarte w systemach informatycznych i teleinformatycznym obsługiwanych przez komornika sądowego i jego pracowników powinny podlegać zabezpieczeniu zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, w szczególności poprzez stosowanie proporcjonalnych środków technicznych i organizacyjnych gwarantujących zapewnienie ochrony przed nieuprawnionym dostępem do systemu. Komornik sądowy jako administrator danych osobowych ma obowiązek każdorazowej weryfikacji tożsamości dłużnika. W przypadku podania przez wierzyciela nieprawidłowych danych dłużnika, w tym nieprawidłowego numeru PESEL, a następnie pozyskania z systemu PESEL-Net danych osobowych w zakresie imienia, nazwiska oraz adresu zamieszkania, komornik sądowy jest obowiązany zweryfikować poprawność uzyskanych danych z danymi otrzymanymi od wierzyciela. Pozyskanie danych osobowych osoby niebędącej dłużnikiem (w wyniku błędu komornika) następuje bez podstawy prawnej. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych komornik sądowy, pozyskując dane z systemu teleinformatycznego, powinien zweryfikować ich poprawność z wnioskiem wierzyciela i w razie wątpliwości zgłosić się do wierzyciela w celu ich poprawienia. Brak działania, o którym mowa w zdaniu poprzedzającym, oznacza brak staranności przy ustalaniu danych dłużnika i naruszenie zasady prawidłowości i poufności (art. 5 ust. 1 lit. d i f RODO). Zasada prawidłowości nakłada na administratora danych obowiązek zadbania o merytoryczną wartość przetwarzanych przez siebie informacji. W RODO podkreślono, że dane osobowe muszą być prawidłowe, a więc rzetelnie weryfikowane co do ich prawdziwości<sup>17</sup>. Komornik sądowy ma również obowiązek zapewnić odpowiednią ochronę środowiska informatycznego, teleinformatycznego przed szkodliwym oprogramowaniem. Jest zobowiązany postępować zgodnie z przepisami prawa, orzeczeniami sądu wydanymi w trybie nadzoru judykacyjnego, zarządzeniami lub zaleceniami uprawnionych organów nadzoru administracyjnego, złożonym ślubowaniem i zasadami etyki zawodowej (art. 25 KomSądU). W myśl art. 27 KomSądU komornik jest obowiązany

<sup>13</sup> A. Klich, Informatyczne instrumenty pozyskiwania informacji przez komornika w postępowaniu egzekucyjnym. Wybrane zagadnienia, PPE 2015, Nr 10, Legalis/el. 2021; K. Flaga-Gieruszyńska, A. Klich, Wykorzystywanie narzędzi internetowych w pracy komornika sądowego, [w:] A. Marciniak, J. Bieluk (red.), Postępowanie i prawo cywilne w dobie informatyzacji, Legalis/el. 2021.

<sup>14</sup> Dz.Urz. UE L Nr 119, s. 1 ze zm.; dalej jako: RODO.

<sup>15</sup> Dz.U. poz. 730.

<sup>16</sup> M. Jabłoński, K. Wygoda, RODO w praktyce funkcjonowania kancelarii komornika sądowego, Sopot 2019, s. 31.

<sup>17</sup> Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 8.10.2019 r. w sprawie nieprawidłowości w procesie przetwarzania danych osobowych Skarżącego przez komornika sądowego, jako danych dłużnika, ZSPU.440.296.2019, <https://uodo.gov.pl/decyzje/ZSPU.440.296.2019> (dostęp z 15.5.2022 r.).

zany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności<sup>18</sup>. Tym samym, biorąc pod uwagę specyfikę działalności egzekucyjnej prowadzonej przez komornika sądowego, stosowane rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informatycznej i bezpieczeństwa środowiska informatycznego powinny być adekwatne do profilu ryzyka kancelarii<sup>19</sup> oraz zabezpieczone przed nielegalnym dostępem oraz podlegać systematycznym, najlepiej niezależnym audytom<sup>20</sup>, a komornik sądowy powinien posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych oraz poprawność działania środowiska teleinformatycznego.

Zabezpieczeniem danych przetwarzanych w zbiorze przed ich ewentualnym zniszczeniem oraz dostępem osób nieuprawnionych jest tworzenie kopii zapasowych i stanowi jeden ze środków mających na celu zapewnienie ciągłości działania kancelarii komorniczej w przypadku wystąpienia awarii systemów informatycznych, teleinformatycznych. Ustawodawca nałożył przy tym na komornika sądowego obowiązek wykonywania dwóch kopii zbiorów zapisów, tzw. kopii zapasowych (ang. *backup*), przy czym każda z wykonanych kopii powinna być przechowywana na oddzielnym informatycznym nośniku danych, odpowiednio zaznaczona oraz zabezpieczona przed zniszczeniem i dostępem osób nieuprawnionych. Zgodnie z § 5 rozporządzenia Ministra Sprawiedliwości z 18.12.2018 r. w sprawie określenia szczegółowych zasad prowadzenia biurowości, rachunkowości i ewidencji operacji finansowych kancelarii komorniczych<sup>21</sup>, kopię zbiorów zapisów komornik sądowy ma obowiązek sporządzić w każdym dniu roboczym. Integralność kopii zapasowych powinna istnieć od momentu jej wytworzenia aż do likwidacji. Przez cały ten okres wykonane kopie zbiorów danych powinny odzwierciedlać stan faktyczny zasobów na moment utworzenia danej kopii, co wyklucza możliwość usuwania z nich jakichkolwiek danych. Należy przy tym podkreślić, że pomimo uchylecia rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych i warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych<sup>22</sup>, podstawowe warunki techniczne, organizacyjne i bezpieczeństwa, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, mogą zostać zastosowane w aktualnych zabezpieczeniach.

Przenosząc rozważania na grunt narzędzi *LegalTech* służących cyfryzacji, digitalizacji, elektronizacji pracy komorników sądowych, innych niż systemy informatyczne, teleinformatyczne służące wsparciu pracy kancelarii komorniczej, zasadnicze znaczenie ma cel przetwarzania informacji, ponieważ to od celu przetwarzania zależy dopuszczalność

korzystania z określonego narzędzia, jak również zakres wykorzystywanych informacji oraz odpowiedzialności związanej z przetwarzaniem danych osobowych. Rozliczalność, wyjaśnialność, prawidłowość, jak też zasady dotyczące przetwarzania danych osobowych uregulowane w art. 5 RODO<sup>23</sup> determinują zakres i sposób realizacji obowiązków informacyjnych związanych z legalnością i bezpieczeństwem przetwarzania danych osobowych<sup>24</sup>. Artykuł 24 ust. 1 RODO zobowiązuje komornika sądowego do wdrożenia odpowiednich środków technicznych i organizacyjnych. Komornik jako administrator obciążony został odpowiedzialnością za przetwarzanie danych osobowych prowadzone w swoim imieniu, jak również przez osoby przez niego upoważnione (działające w jego imieniu), a w szczególności za implementację systemu wdrażającego środki zapewniające zgodność przetwarzania danych osobowych z RODO i proporcjonalnie, biorąc pod uwagę kontekst, zakres, cel przetwarzania danych oraz ryzyka dla praw i wolności podmiotów danych<sup>25</sup>. Podjęcie odpowiednich środków bezpieczeństwa w zakresie dostępu do narzędzi i systemów informatycznych używanych w kancelariach zwiększa ochronę w razie wycieku danych<sup>26</sup>. Zatem zapewnienie bezpieczeństwa powinno być obowiązkiem każdego pracownika kancelarii komorniczej. Odpowiedzialność za ochronę informacji i bezpieczeństwo warto wprowadzić zarówno do umów pracowniczych, jak i do umów zawieranych z dostawcami, z których usług kancelaria komornicza korzysta. Warto jednak zwrócić uwagę, aby obowiązkom nałożonym na pracowników kancelarii towarzyszyła stosowna wiedza zdobywana w czasie kursów i szkoleń. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapoznana z przepisami dotyczącymi ochrony danych osobowych. Istotne jest przy tym, aby szkolenia odbywały się cyklicznie celem aktualizowania wiedzy zaplecza osobowego. Jak słusznie zauważa

<sup>18</sup> Przedmiotowy obowiązek trwa także po odwołaniu komornika z zajmowanego stanowiska albo wygaśnięciu powołania na stanowisko komornika z mocy prawa, z wyjątkiem, gdy komornik składa zeznanie jako świadek lub strona przed sądem lub prokuratorem, chyba że ujawnienie tajemnicy zagraża dobru państwa. W tym przypadku od obowiązku może zwolnić komornika Minister Sprawiedliwości.

<sup>19</sup> I. Piankowska, N. Stojanowska, K. Maciejewska, komentarz do § 5, teza 10, [w:] M. Jaranowski, N. Stojanowska (red.), Szczegółowe zasady prowadzenia biurowości, rachunkowości i ewidencji operacji finansowych kancelarii komorniczych, Warszawa 2021, s. 64.

<sup>20</sup> M. Sztandur, Odpowiedzialność komornika za naruszenie przepisów o ochronie danych, Nowa Currenda 2018, Nr 7, s. 36.

<sup>21</sup> Dz.U. poz. 2517.

<sup>22</sup> Dz.U. Nr 100, poz. 1024.

<sup>23</sup> Zasada zgodności z prawem, rzetelność i przejrzystość.

<sup>24</sup> D. Lubasz, Rozdział XIII. Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji, [w:] L. Lai, M. Świerczyński (red.), Prawo sztucznej inteligencji, Warszawa 2020, s. 179.

<sup>25</sup> D. Lubasz, komentarz do art. 24, teza Nr 2, [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 586.

<sup>26</sup> M. Sztandur, Odpowiedzialność komornika..., s. 36.

R. Pająk, wspominając o rolach i odpowiedzialności, należy zwrócić szczególną uwagę, aby każdy pracownik miał dostęp wyłącznie do informacji niezbędnych mu do wykonywanej pracy. Zasada wiedzy niezbędnej (ang. *need to know*), czasami nazywana również zasadą wiedzy koniecznej/uzasadnionej, pozwala zminimalizować skutki naruszeń bezpieczeństwa. Dodatkowo wszelkie użytkowane narzędzia powinny zostać skonfigurowane w sposób umożliwiający jednoznaczne zidentyfikowanie osoby odpowiedzialnej za każdą akcję (tzw. rozliczalność, ang. *accountability*)<sup>27</sup>.

Przechodząc do środków bezpieczeństwa stosowanych w kancelarii komorniczej przy wykorzystaniu narzędzi *LegalTech*, należy mieć na uwadze zasady bezpiecznego użytkowania sprzętu informatycznego, programów, politykę haseł, zasady korzystania z poczty elektronicznej, Internetu, stosowanie ochrony antywirusowej.

Zasady bezpiecznego użytkowania sprzętu informatycznego stanowią regularne aktualizowanie systemu operacyjnego i oprogramowania, zarówno na komputerach, jak i urządzeniach przenośnych, a także wszelkich innych urządzeniach elektronicznych, skonfigurowanie mechanizmów bezpieczeństwa w przypadku pracy w środowisku chmurowym, korzystanie z uwierzytelnienia dwuskładnikowego/wieloskładnikowego (ang. *two-factor/multi-factor authentication*), aplikacji służących do uwierzytelniania użytkownika, korzystanie z rozwiązań typu VPN (ang. *Virtual Private Network*), wyłączenie możliwości podpinania nośników typu USB przez osoby trzecie, szyfrowanie danych na wszystkich nośnikach i urządzeniach za pomocą algorytmów, haseł, automatycznego skanera, pseudonimizację danych osobowych zapisanych na nich. Podkreślenia przy tym wymaga, że nośniki danych zawierające dane osobowe powinny być przechowywane w miejscach o ograniczonym i kontrolowanym dostępie, a każda osoba działająca z upoważnienia komornika sądowego jako administratora i mająca dostęp do danych osobowych jest zobowiązana przetwarzać je wyłącznie na polecenie administratora (art. 29 RODO).

Polityka haseł obejmuje korzystanie z różnych haseł dla każdego serwisu, zakaz stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów, definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca, stosowania haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca bądź inny możliwy do odgadnięcia klucz, korzystanie z „menadżerów haseł”<sup>28</sup>, zakaz ujawniania hasła innym osobom (hasło powinno pozostać w poufności, nawet po utracie przez nie ważności).

Do zasad bezpiecznego korzystania z poczty elektronicznej należy zasada zwracania szczególnej uwagi na poprawność adresu odbiorcy dokumentu, zakaz konfigurowania kont służbowej poczty elektronicznej do automatycznego przekierowania wiadomości na adres zewnętrzny oraz zgłaszanie ad-

ministratorowi przypadków podejrzanych wiadomości e-mailowych. Należy przy tym wskazać, że pracownik kancelarii bez zgody komornika nie ma prawa wysłać korespondencji zawierającej dane osobowe pracodawcy, jego pracowników, dostawców za pośrednictwem Internetu, w tym przy wykorzystaniu prywatnej elektronicznej skrzynki pocztowej.

W kwestii ochrony antywirusowej, użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe, a w przypadkach stwierdzenia zainfekowania systemu informatycznego, teleinformatycznego użytkownik zobowiązany jest poinformować niezwłocznie o tym fakcie komornika sądowego lub osobę przez niego upoważnioną.

Odnosząc się natomiast do zasad korzystania z Internetu, istotne jest używanie innej przeglądarki do łączenia się z bankiem, kancelarią komorniczą czy stronami internetowymi, gdzie posiada się dostęp do poufnych danych, a także korzystanie z Internetu wyłącznie w celach służbowych. Zakazane jest wchodzenie na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo. Istotne jest również zachowanie szczególnej ostrożności w przypadku podejrzanego żądania lub prośby zalogowania się na stronę internetową (np. na stronę banku kancelarii komorniczej czy też poczty e-mailowej).

Bezpieczeństwo danych w kancelarii komorniczej, ochrona informacji, przetwarzanie danych osobowych to proces. Zarządzanie bezpieczeństwem powinno być na bieżąco aktualizowane i rozwijane w zależności od produktów, usług i narzędzi *LegalTech* wykorzystywanych w kancelarii. Środki ochrony przetwarzania danych osobowych powinny być dostosowane do skali ryzyka, zagrożeń i charakteru przetwarzanych danych, natomiast ocena dostosowania powinna następować pod kątem poufności, integralności i dostępności danych, biorąc przy tym pod uwagę ich zakres, kontekst i cel przetwarzania, a tym samym także kwestie zapewnienia bezpieczeństwa usług przetwarzania (niezawodność, integralność i dostępność do systemu przetwarzania) oraz zapewnienie autentyczności i rozliczalności danych i podmiotów uczestniczących w przetwarzaniu<sup>29</sup>.

<sup>27</sup> R. Pająk, Rozdział 5. Bezpieczeństwo danych w kancelariach prawnych, [w:] D. Szostek (red.), *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji*, w tym w kancelarii oraz dziale prawnym, Legalis/el. 2021.

<sup>28</sup> Programów, które pozwalają składować i generować unikalne hasła dla każdego użytkowanego serwisu internetowego oraz mogą dodatkowo dbać o to, aby hasło było uzupełniane tylko na poprawnej stronie.

<sup>29</sup> Jak zrozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1. Maj 2018, s. 5, <https://uodo.gov.pl/pl/123/208> (dostęp z 13.11.2021 r.).

## Podsumowanie

Postęp technologiczny determinuje zmiany w obszarze zawodów prawniczych. Nowoczesny komornik sądowy nie może funkcjonować bez wsparcia zaplecza osobowego, narzędzi, systemów informatycznych, teleinformatycznych czy też systemów eksperckich wspierających jego pracę, w tym pracę kancelarii komorniczej. Nowe technologie są sposobem na zwiększanie efektywności procesów prawnych. Jednak wśród istotnych czynników ograniczających wykorzystanie *LegalTech* w pracy kancelarii komorniczej jest brak dostępu do narzędzi dopasowanych do konkretnych procesów, brak kalibracji narzędzi na potrzeby języka polskiego, nieprzystosowanie rozwiązań globalnych do specyfiki lokalnej, czas wymagany do zapoznania się z narzędziem i jego skuteczne wdrożenie w kancelarii, brak łatwego dostępu do informacji o funkcjonalności narzędzi technologicznych w branży

prawniczej, bariery mentalne – niechęć do zmian i uczenia się nowych rozwiązań przez komorników sądowych i pracowników. Wdrażanie *LegalTech* w kancelariach komorniczych jest koniecznością oraz kolejnym etapem rozwoju technologicznego. Stanowi przy tym wyzwanie związane ze zwiększonymi inwestycjami, reorganizacją standardowego modelu działania kancelarii, poszukiwaniem efektywności czasowej pracy oraz bezpieczeństwem przetwarzania danych osobowych, realizacją obowiązków związanych z wymaganiami nałożonymi przez RODO. *LegalTech* wymaga rozpoznania analizy ryzyka, rozliczalności, ochrony tajemnicy zawodowej, a aktualne podejście do zgodności w zakresie bezpieczeństwa informacji wskazuje na celowość i sensowność regularnego monitorowania wymaganych parametrów bezpieczeństwa, dostosowanych do zmieniających się warunków organizacyjnych kancelarii komorniczych.

**Słowa kluczowe:** sztuczna inteligencja, nowe technologie, kancelaria komornicza, komornik sądowy, legaltech, postępowanie egzekucyjne, ochrona danych osobowych, cyfryzacja, elektronizacja.

---

## *LegalTech* in bailiff offices

*Transformational technologies are used to digitize the work of court bailiffs. They are a way to increase the effectiveness, productivity, and efficiency of legal processes. A modern bailiff cannot function without the support of information systems, ICT systems, or expert systems. The author presents the organization of the work of bailiff offices, the possibilities offered by LegalTech, and the possibilities of using IT tools in the work of bailiff offices. Particular attention was paid to the security of personal data processed in bailiff offices, the security measures applied, and security management. The article aims to indicate that the implementation of LegalTech in bailiff offices is a must. It is a challenge related to increased investments, reorganization of the offices' operating model, the search for efficiency in working time, or the security of personal data processing, and requires the recognition of risk analysis, accountability, and protection of professional secrecy.*

**Keywords:** Artificial Intelligence, new technologies, bailiff's office, bailiff, LegalTech, enforcement proceedings, personal data protection, digitization.

---



**Monografie Prawnicze**

ksiegarnia.beck.pl  
Zadzwonić: 81 46 13 300  
E-mail: kontakt@beck.pl

  
C.H. BECK