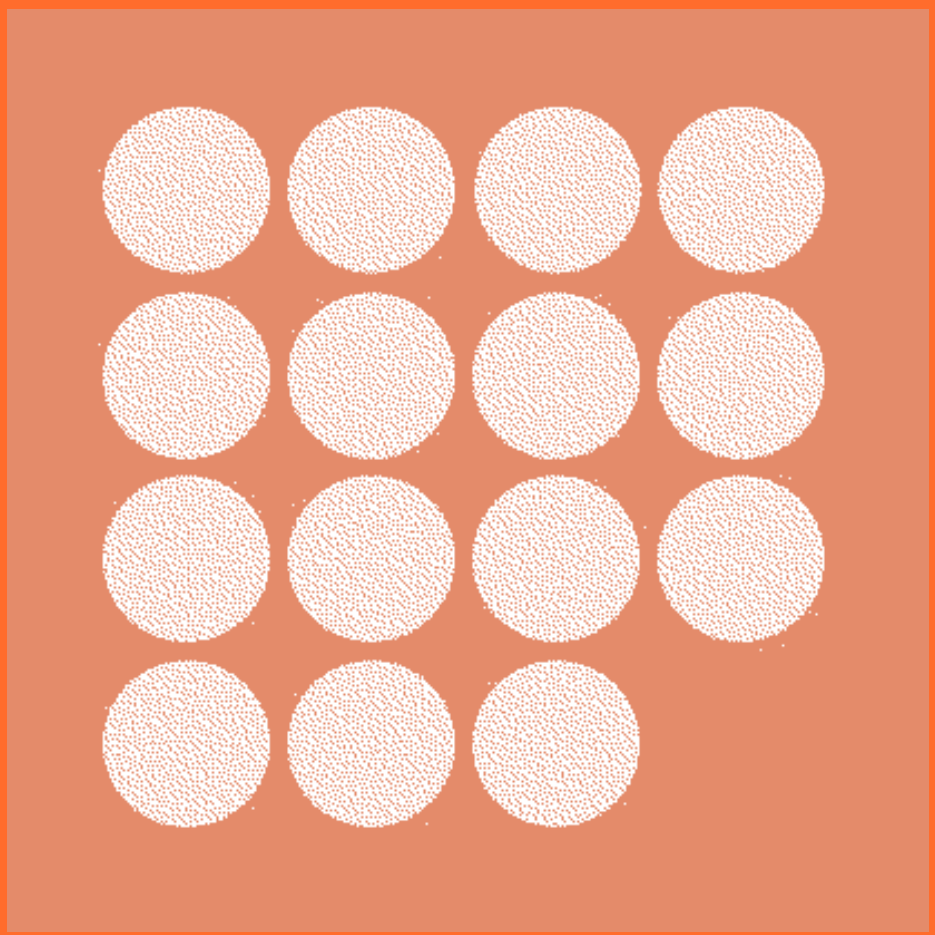
VOL. II



Innovations

Published in conjunction with the debate "The right to unplug: Dignity, privacy and new technologies," organised by Wardyński & Partners as part of the celebration of the firm's 30th anniversary.

Substantive editing: Krzysztof Wojdyło
Editing: Justyna Zandberg-Malec
Translation: Christopher Smith

Contents

Tomasz Wardyński
Krzysztof Wojdyło

Technology and its discontents

Any new technology that gains universal application changes the existing world. The reconfiguration occurs imperceptibly but thoroughly. But in this new reality, how should the rule of law, values essential to the civil society and human rights be protected?

A new economic reality functioning in cyberspace has arisen before our very eyes. Human activity, both positive and negative, is moving to the virtual arena that functions above and beyond state borders. Consequently we must develop the skill to adapt familiar legal institutions to this new reality.

The interdisciplinary New Technologies practice has functioned at our law firm for several years. The lawyers on the team share a passion for examining technical issues and their influence on the possibility of effectively protecting the rights of citizens and the civil society—and a belief that lawyers must raise their awareness of new technologies.

A time of technological revolution

Innovation is a keyword today organising social and economic life. Governments and enterprises create innovation strategies. Startups attract unprecedented attention. In the information buzz it is easy to lose sight of the deeper meaning of the ongoing transformation.

Technologies fundamentally change us. They are not socially, economically or culturally neutral. Considering the pace and scale of changes, reflection on new technologies remains inadequate. When we abandon deep reflection, we expose ourselves to the risk that many changes will pass us by unnoticed, depriving us of the opportunity of responding to them.

As lawyers, we regard it as particularly vital to properly grasp the interrelationship between law and technology. We know that in the years ahead, the

law faces the huge challenges of regulating artificial intelligence, blockchain, and genetic engineering. This doesn't mean the simple regulation of a new field of reality. Many new technologies can fundamentally alter the paradigms that form the foundation for contemporary legal systems. They can change the meaning of law, how it is created and enforced. How the legal profession is practised will also unavoidably change. Therefore we lawyers will also have to change.

Law constantly chasing reality

The interrelationship between law and technologies is often dismissed with the claim that the law cannot keep up with reality. But there is an essential truth lurking in this statement. More and more aspects of reality escape colonisation by the law.

We have grown accustomed to living in a world in which the great majority of our fields of activity are subject to rules sanctioned by traditional sources for creation of law. This may generate frustration but also provides a sense of certainty, stability and control over reality. By giving ground to new technologies, we begin to lose that control.

The point is not that there are no rules at all in new areas of reality. But the rules are created differently then we have grown used to. The most important rules for functioning of the internet, continuing to shape life online, were not created by any legislature in the traditional sense, holding democratic legitimacy for creating law. Nor were these rules the subject of any democratic public debate.

New areas of reality highlight the growing importance of technical standards and instruments of "soft law" like guidelines, recommendations and best practices. It appears to us crucial that lawyers become aware of this process and quickly begin to take an active part in alternative lawmaking processes.

Progressive complication of the system and internal contradictions

Technological progress is accompanied by the growing complexity of the legal system. Every new field will sooner or later become the subject of regulations, whether enacted traditionally or adopted through an alternative method of law creation. Thirty years ago there were no regulations governing the internet. Twenty years ago there were only rudimentary provisions governing electronic payment services—a field now controlled by dozens of acts and hundreds of provisions of law.

A consequence is a growing number of interdependencies as well as conflicts between individual elements of the legal system. Regulations drafted

without regard for the broader context lead to internal inconsistencies within the system. No doubt such situations will only grow increasingly common.

A system riddled with internal inconsistencies cannot ensure a sense of legal certainty or justice. This makes legal services increasingly expensive and inefficient. Resolution of judicial disputes will be increasingly time-consuming and require more involvement of expensive experts. In the short term this situation seems attractive for lawyers. But over the longer term, it is highly disadvantageous for the society and the economy. More than ever, legal assistance may become accessible only for the few.

We thus face the question of the model for further development of the legal system. The existing model has generally led to creation of successive regulations in reaction to the development of new technologies. This leads to further expansion and complication of the legal system, making it increasingly dense and non-transparent. This threatens a loss of control over the totality of the system and an increase in social frustration generated by the lack of transparency in the system of laws.

This makes it urgent to take a creative effort toward developing alternative solutions. A departure from the existing paradigm under which the law must regulate in detail every new field of reality may come into play, as well as the development of tools (e.g. based on artificial intelligence) enabling more effective identification of inconsistencies within the system.

Challenge 1: blockchain

Blockchain has the potential to create a truly global space for exchange of goods and services with an architecture that prohibits the presence of a sovereign. This is because blockchain is a distributed register maintained by independent entities spread all over the globe, over which, as a rule, no one exerts control.

It may be said that what happens in blockchain occurs both everywhere and nowhere. We cannot point to any specific legal order governing particular actions or transactions playing out in this space.

In this context, the rapid growth of smart contracts must also be mentioned. This concept refers to legal relations governed not by a traditional contract drafted in natural language, but by a contract taking the form of computer code. Such a contract may be concluded and executed automatically. Solutions based on smart contracts are commonly used in blockchain.

Blockchain raises many challenges for the traditional legal system. Guarantees of safety and justice must be created in this "new jurisdiction" where code is law. Here lawyers have a vital role to play. But to rise to this

challenge, they will have to cast aside many of their existing habits and acquire entirely new skills.

Challenge 2: autonomous algorithms

Algorithms are already involved in many decision-making processes. They process vast quantities of data and make decisions at a speed that cannot be matched by humans. Along with the growth of technology, they are increasing their degree of autonomy. And this is what generates the most challenges for the legal system.

The logic of decision-making by autonomous algorithms is often opaque or misunderstood by people. Nonetheless, because of the efficiency of these algorithms, we are willing to cede to them control over many areas of life. Algorithms are already evaluating creditworthiness and taking investment decisions. In the near future we will give them control over transportation, logistics services, and even healthcare.

As a new factor or agent contributing to creation of our reality, algorithms may become a kind of entity vested with rights and obligations. Their actions cannot be clearly ascribed to specific persons. Even the creators of autonomous algorithms are incapable of predicting their logic or behaviour.

Within the next few years, the legal system will have to address this phenomenon. It does not seem that the traditional approach involving identification of the human agent tied to an autonomous algorithm and bearing liability for its action will work. We must seek non-standard solutions that reflect the nature of new agents in our reality.

Challenge 3: cybercrime

Although we learn about new cyber offences nearly every day, we are still not wholly aware of the importance of this phenomenon. Cybercrime clearly reveals the impotence of the traditional legal system in the era of new technologies. The detection rate for cyber offences remains negligible. A huge percentage of investigations are discontinued because of failure to identify the perpetrators.

This is due to numerous factors. First, cybercrime is generally international in scope, requiring coordinated action by law enforcement authorities from multiple jurisdictions. But in many such cases the system of international legal assistance is highly inefficient, requiring victims of cyber offences to incur high legal costs with no guarantee of success. Second, the battle against cybercrime requires highly specialised knowledge and the supply of appropriate specialists is limited. This translates into high costs for preparing evidence and expert analyses and drags out the length of the proceedings.

The low detection rate for cyber offences and the growing number of helpless victims left to their own devices represents civilisational and legal regression. Here too there is an urgent need for paradigm change and a new way of acting, as traditional methods are failing and there are no prospects for improvement in the near future. Without a new approach, we are at risk of a growing sense of anarchy and even a retreat from the use of new technologies.

Challenge 4: lawyers in a new reality

We anticipate that automated solutions will provide support for us in legal practice to a much greater extent than is now the case. This will make it easier for us to identify the appropriate legal standard and properly apply it to the given state of facts. Perhaps this process will soon occur to a large degree without the involvement of lawyers. This will change the essence of our profession.

This will emphasise the key skill of decoding the deeper, humanistic meaning of reality. It is in this process that we perceive the essence of the legal profession in the future. It is only thanks to a humanistic perspective that we will be in a position to regulate new aspects of reality in a manner that preserves human dignity and justice. Only a humanistic perspective will enable us to take a holistic view of reality and identify the meaning and significance of increasingly complex legal norms.

Teaching these skills will undoubtedly require changes in legal education. Assimilation of law by rote memorisation will play a smaller and smaller role in the process, as it is a waste of energy when machines can identify the relevant regulations. We should place a greater stress on processes that teach lawyers to understand reality, stir intellectual curiosity, and foster a humanistic perspective on the world. The education process should also develop the knowledge and skills necessary to understand the technical aspects of the functioning of new technologies.

Conclusions

In the reality that surrounds us, it is our professional responsibility to foster and maintain our fundamental values, including human dignity and justice. We have traditionally assumed that the threats to these values emerge primarily from oppressive political systems. But dynamic growth of technology has generated an additional source of threats, which left to itself can lead to creation of a dehumanised reality.

That is why we as lawyers must pay increasing attention to new technologies. Meeting the challenges which technology poses for society, culture and policy

requires collective effort by the legal community aimed at developing new skills among lawyers, and a new approach to practice of the legal profession.

Tomasz Wardyński
adwokat, founding partner

Krzysztof Wojdyło
adwokat, partner in charge of the New Technologies practice

Agnieszka Kraińska

Freedom from the internet

The freedom of access to the internet and freedom on the internet are guaranteed in EU law by, among other things, the principle of net neutrality. The internet is treated as a public service, and the lack of privileging of transmission guarantees equal access to content. The right of access to the internet is an expression of the human right to freedom of opinion and expression (enshrined in Art. 19 of the Universal Declaration of Human Rights and Art. 10 of the European Convention on Human Rights), the importance of which is beyond debate.

We must not lose sight of the flipside of the internet, however, i.e. the harvesting of users' data on a mass scale. Such data have huge value and can be exploited in many ways, including by the public administration, which more and more often employs information and communications technologies. The slogan "e-administration" covers issues associated with e-identity, electronic ID cards, and technologies for scanning citizens' faces, retinas, and fingerprints. Considering the risks connected with the use of such data, the concept of a right to refuse to participate in online life—freedom from the internet—appears tempting. Is exercise of this right, in a negative sense, possible at all, or will it still be possible in the near future?

The premise of such a freedom may sound controversial, particularly in a world where the concern of governments, NGOs and international organisations like the EU and the UN is focused more on the problem of digital exclusion. I will nonetheless attempt to show that the demand for freedom from the internet is entirely justified. The right to privacy enshrined in Art. 12 of the Universal Declaration of Human Rights and Art. 8 of the European Convention on Human Rights may be regarded as a guarantee of such a freedom.

Privacy and liberty

Many novels and films terrify us with the vision of a dystopian society stripped of privacy. After all, privacy is fundamental not only at the individual level, for also for the existence of liberal democracy.

The personality of each one of us is shaped socially, starting from infancy. But individuality and personal development require a zone of privacy and the ability to establish personal boundaries. A subjective sense of self and critical thought are formed between the public and private spheres. There is a reason that totalitarian systems seek to minimise the sphere of human privacy. Continual control over the individual facilitates ongoing influence over behaviour and shaping of personality.

Meanwhile, the contemporary technological civilisation is increasingly a civilisation of fragmented attention and unceasing stimuli, where there is no time for moments of reflection. The reality surrounding us is studded with electronic devices monitoring our everyday activity and preferences. On social media, we voluntarily turn over information on vast areas of our personal life.

Many internet users still don't realise that their activity on the web shapes the feedback they receive from it. Search engines filter and rank results by tailoring them to what they know about the searcher. In this sense, both search engines and our circle of friends on social media with whom we share a common world view confirm us in our belief that the world is the way we think it is. The tools we use to explore the world around us shape our understanding of that world.

The traces of data we leave online enable search results to be suited to our needs and preferences. That is certainly convenient. But it must be remembered that when moving our activity onto the internet and placing greater and greater weight on social media, we risk losing our clear-headed assessment of the surrounding reality.

Voluntarily relinquishing privacy in favour of convenience and security limits the ability to shape our critical thinking and independence—in other words, in some sense it means relinquishing our liberty.

Privacy and democracy

The sphere of comfort generated for us by the world wide web does not come for free. We pay for it with information about ourselves. On an individual level, waiving our privacy may dampen caution, criticism, and creativity. It also has far-reaching consequences at the societal level.

A democratic society cannot exist without aware and active citizens. Citizens shape political and economic institutions, and these institutions in turn shape individuals and the society they live in. Liberal democratic states and market-economy institutions are the fruits of long-term processes and experiences, but their citizens accept the norms and rules governing such societies as natural. Diverse examples show that liberal democracy cannot be grafted onto societies that are not ready for it.

waiving our privacy may dampen caution, criticism, and creativity

The technological change introduced by the internet has enabled unprecedented changes in access to information and communications technologies. These new tools are created by us, but they also shape us, in the sense that we perceive the world around us through these tools. To visualise this influence, it's enough to compare an automobile journey with GPS navigation and without it. Research shows that the use of electronic devices alters the functioning of the brain, and a person using an electronic device functions differently in everyday life.

Moreover, we increasingly use tools whose functioning we do not understand at all. Such devices use internet connections to facilitate ongoing supervision and monitoring of human activity. This supervision is not tied to a totalitarian political system, but to the growth of capitalism (commercial information) and the contemporary nation state (security policy).

Thanks to the proliferation of the internet of things and the internet of people, this supervision over human activity is becoming omnipresent, routine and systematic, and the type and intensity of this supervision are shaped in response to the monitored activity.

It is correctly pointed out that this type of discreet and constant supervision is much more effective than the open and brutal oversight in non-democratic countries. Moreover, non-democratic states are eager to employ state-of-the-art tools and introduce constant monitoring of the society, as demonstrated for example by recent reports on the widespread use of face recognition technologies in China.

Liberal democracies routinely collect and use data for purposes of national security, as demonstrated for example in the proceedings against the British government by Privacy International (e.g. concerning mass harvesting of telecommunications data by British intelligence).

Information about us is also invaluable in a commercial sense, and the appetite for data of firms like Google and Facebook is insatiable. They use information about consumer preferences for profiling of ads, search results, and other content, and the information is also sold on to others. Data left online are extremely useful for setting prices, managing risk, and profiling potential customers.

It is striking in this context that in Western societies, consumers voluntarily and actively take part in this process of monitoring. They regard personalisation of information, a sense of security, access to better products and more interesting offers, or higher visibility on social media as adequate compensation for the incursions into their sphere of privacy. There is even talk of personality being defined as a permanent presence in social media.

For reasons best explored by psychologists, presence on social media is based on strong emotions. These emotions do not foster in-depth discussion, but are reduced to a wave of likes and hate. Moreover, limiting contacts between people with differing views eliminates discourse and confrontation of opinions. Public debate ceases to exist, as it requires both discomfort and deep reflection. And citizens existing in a personalised bubble, constantly stimulated by new information and images, have no desire to take part in such a debate, no need to step outside their comfort zone, but wall themselves up within their own "tribes."

Even more seriously, citizens living in a world of digital technology are not only subjected to constant monitoring, but are also more susceptible to manipulation by false information, as demonstrated by such cases as the Cambridge Analytica scandal.

The loss of the privacy essential for critical thinking thus poses a threat to liberal democracy.

Privacy and innovation

A society lacking in debate, where citizens live in bubbles created by social media, is not a society that fosters innovation.

Privacy is a necessary condition for innovation, because innovation requires critical thinking and room for experimentation and failure. Innovation arises out of wrestling with a problem and finding a creative solution to the problem. It requires meeting with people who think differently, and contact with new ideas. An innovator cannot thrive under the tyranny of transparency and permanent judgment connected with a constant online presence.

True, some do take the view that innovation can exist without innovators—for example as a result of automated crunching of huge quantities of data. But the tool of Big Data should not be confused with innovation. Humans must define the scope of the research and interpret and apply the results.

What next?

These ruminations aren't designed to show that the internet is a bad thing. On the contrary, the internet provides access to information and the exchange of thoughts on an unprecedented scale. But any tool—in this case a tool of global reach—also gives rise to unanticipated risks and threats. The revolution associated with universal access to the internet has been underway for only two decades, and we are all still learning how this impacts our lives, the society around us, and our reality.

Ensuring universal access to the internet and digital technologies may paradoxically deepen class divisions and lead to huge inequalities in the quality

of information people have access to, and in the possession and exploitation of data obtained from people. We must not lose sight of the relentless pressure caused on one side by the commercial dimension of the internet and efforts to eliminate net neutrality, in the sense of equal access to information, and on the other side by security policy and attempts at exercising universal control. These dimensions are interrelated in various aspects.

A consequence of the loss of privacy and unequal access to information may be the development of a small, privileged group of individuals exercising power on the internet over huge ranks of manipulated people reduced to the role of generating data to feed the system.

I don't believe it is possible anymore in Western society to entirely exclude oneself from the internet without also being excluded from normal functioning. But uncritical digital inclusion leads to a world where, as Dave Eggers put it in his dystopian novel *The Circle*, "Secrets are lies. Sharing is caring. Privacy is theft."

Finding a golden mean and properly delineating boundaries is a huge challenge for democratic societies. Education on having a critical presence in e-reality is essential, along with appropriate regulations ensuring individual and social control over capturing and processing of data by the state and the private sector, and guaranteeing equal access to information. In this respect I see room for reasonable state intervention and for international cooperation, without which these measures will not achieve the desired results. In my view, nation states are not in a position to deal individually with these threats, which like the internet itself are supranational and respect no boundaries.

Agnieszka Kraińska
attorney-at-law, EU Law practice

privacy is a necessary condition for innovation

Pioneering beginnings

Włodzimierz Szoszuk
talks with Justyna Zandberg-Malec

Today the law firm advises on matters involving blockchain, cryptocurrencies, cybercrime.... How did it look 30 years ago?
The beginnings were totally pioneering. We began during the transformation from the communist system, at the beginnings of democracy and the free market. Poland was opening up to foreign investment and becoming an attractive sales market for products that hadn't existed here before, as well as a location for quickly growing native industry. As a small firm, we faced a flood of assignments from all corners of the world, concerning all fields of law.

Moreover, the process of reforming the law could not keep up with the systemic changes. That created challenges for lawyers.

Every assignment was like tailoring a bespoke suit. It was interesting but took a lot of time. It was only after handling several similar matters, transactions, the first litigation cases, that we could begin to develop a kind of workshop for our craft, where after achieving fluency you could even become an artist.

So the atmosphere resembled what we might find today in a tech startup?
To a certain degree, yes. We knew our core activity, but the whole business environment, the demands of the market and clients, were new to us. We were lucky, however, that the western law firms who assigned work to us shared their know-how with us. We learned on the go how to work with them, how to understand our clients' business goals, how to tailor them to suit the Polish realities. We were just learning how to fill the role of a business adviser. The norm previously had been that a lawyer lived and breathed in a world of regulations, not commercial realities.

Fortunately there were many opportunities to raise our qualifications and hone our skills. If you knew the language, you could go abroad for study or an internship. There were organisations sponsoring stipends, exchange

programmes. Lawyers from the West came to observe how the situation was evolving, and we could visit western firms. I practised for several months in an English firm, and later an American one, returning with an entirely new vision of how to handle cases and operate a law firm.

We also learned a new way of writing. Once upon a time lawyers thought that before reaching a conclusion, they had to instruct the client on the law. They would quote five articles for the client, place them in a broader context, explain their purpose, and only then, after building up the tension, lead the client to the conclusion relevant to their own business. That was a waste of time for us and for the client. It was in my foreign internships that I encountered entirely different texts, addressing an issue without regurgitating chapter and verse of the regulations. They stated the grounds and conditions, but detached from dense legal matter. That was a revolution.

The instructional school of writing still had a purpose in the case of the courts. The judges were also not well-oriented in the new reality, and thus, for example, the first trademark infringement claims were couched like a treatise: what is a trademark, what is its scope of protection, the catalogue of possible claims, how they can be enforced. We had to subtly and gracefully explain to the judge how to handle a new type of case for the first time.

External legal opinions were also common in those days. If something was doubtful or not entirely clear in Polish law, we had to consult a legal scholar, authors of commentaries, to provide an opinion helping us present our argument to the judge more persuasively. There is no longer any rationale for that approach. Today the argumentation to the court is more concise and focused on the specific legal issue requiring adjudication.

What were the realities of a lawyer's work 30 years ago?

First and foremost, we worked at a different tempo, much more slowly—which doesn't mean we had more time. Lots of time was taken up with activities that today barely require our attention.

I remember that we had a long investment contract to translate, several hundred pages. There were no translation agencies yet. We just split up the work among a dozen people at the firm and worked on the translation at home, in the evenings. Computers existed then, but there was no email—that appeared much later. Texts were stored on floppy disks. We corresponded by post and fax. Photocopiers were still revolutionary, spreading from the mid-1980s. There was no internet, obviously—like email, that did not reach the firm until 1998. Even then, it would be several years before any useful content appeared online. It wasn't until around 2003 or 2004 that an internet connection really began to provide access to data and information from all over

the world. Then the pace of work naturally picked up. On top of that, the firm itself was growing, and we had more work than we could handle.

How did the Intellectual Property practice begin?

I should first mention the late Prof. Irena Wiszniewska-Białecka, who died in 2018[1]. She built this practice. I joined the practice after she had been running it for two years, and we worked together for many years. We were also quickly joined by other people.

The first cases in our field were so fascinating because the Polish market was flooded with products from other countries. It was totally wild imports, unorganised, and distribution channels did not yet exist. Suddenly pirated and counterfeit goods appeared, infringing copyright and industrial property rights. Trademarks and principles of fair competition were violated on a massive scale. It was our job to defend these rights on behalf of our new clients. We initiated the first trademark protection proceedings. We attempted to take advantage of instruments provided for in civil procedure, such as interim relief to secure claims. These were things that hardly existed in Polish practice at the time. During the post-war era, until 1989 there had been one only trial for trademark protection. The court in that case ordered interim relief by seizure of goods infringing an American trademark for clothing. Today in the course of a year we probably file more than a dozen applications for interim relief. This shows that intellectual property protection started from practically nothing.

The level of social awareness was probably even less. It was a time when cassettes were sold from cots and there were openly functioning establishments in the business of copying discs.

Piracy indeed flourished. The market was so starved that there was an outlet for practically anything. Infringers took advantage of the vacuum, a period of slow protection. They had no way of knowing whether the firm whose rights they were infringing would enforce its intellectual property rights in Poland. This situation continued until the mid-1990s. After that protection picked up steam and reached a level comparable to that in more developed countries. Before EU accession Poland had to bring its laws into compliance with EU standards, so legal reforms moved quickly. Now Polish judges and

1 From the beginning of 2001 Prof. Wiszniewska-Białecka served as a judge of the Supreme Administrative Court of Poland, and from 2004–2016 as a judge at the Court of First Instance (subsequently the General Court), part of the Court of Justice of the European Union in Luxembourg.

Polish courts issue excellent rulings, which our colleagues from the West often cite.

When did Polish clients appear? I understand in the beginning your clients were mostly western rightholders.

In my own field Polish clients appeared quite late. But sometime around 2000 Polish business began to respond rapidly to the new economic environment, and dynamic Polish firms arose and quickly gained a position on the market. They knew that in a dispute with large corporations they had to have proper legal representation, and because they knew us often from the opposing side, they also sought our help. We had the pleasant awareness that we were helping the developing Polish economy, Polish business.

All of this today sounds like ancient history. It's strange to think that we're talking about realities from just two decades ago, or even less. Today young lawyers are much better prepared for their role. But they cannot rely on the kind of credit we could. Clients then realised that certain things had not yet been organised in Poland. Today investors expect the same from a young Polish lawyer as they would from a young Belgian, Dutch or Finnish lawyer.

It's also obvious that lawyers must think in business terms. The highest compliment for a lawyer is to hear from the client, "My lawyer thinks like I do."

In today's world, particularly in the field of new technologies, the realities change faster and faster. By its nature, the law lags behind. That's why lawyers must be prepared to face ever new challenges.

Włodzimierz Szoszuk
adwokat, partner in charge of the Intellectual Property practice

Interview conducted by Justyna Zandberg-Malec

the highest compliment for a lawyer is to hear from the client, "my lawyer thinks like I do"

Lawyers in a world of new technologies

Tomasz Wardyński talks with Justyna Zandberg-Malec

What has changed in the practice of the legal profession over the 30 years the firm has been existence?

Everything and nothing. The role of the advocate—from the beginning of the profession in ancient Rome—is first and foremost to relieve the client of the stress connected with the legal difficulty the client finds himself in, through his own neglect or lack of knowledge, or infringement of his rights by the state or a counterparty. From this perspective, nothing has changed. Nonetheless, the professional environment has changed radically.

Today we practise our profession in an entirely different economic, social and technical reality than 15 or 20 years ago. Technologies have changed, but so have the needs and expectations of clients. Technologies generally facilitate work and save time, but they also speed up reality. With the advent of the fax machine, we began to answer letters the same day, and since email came along we respond to inquiries and correspondence within two to four hours, or by the end of the day at the latest. Response time is also treated as a major indicator of quality. As we respond quickly, we receive more inquiries and matters from clients. Thus as a result of technological change we are confronted with a workload exceeding what one person can handle, and we begin to work in larger and larger teams.

A similar effect has been generated by the huge commercial transactions that have shaped the market, as well as all the processes connected with these transactions. These have also in some sense forced people who practised the profession singly or in small teams to expand their teams, because they now have to deal with issues crossing multiple disciplines. As we know, a single mind can master at best perhaps one or two disciplines. When the issue grows more complicated, we must put our heads together. Once upon a time we handled this by consulting colleagues on a case-by-case basis. Today the legal landscape is dominated by big firms.

Of course the size of the firm also affects how the profession is practised. Larger firms are more corporate than smaller ones, and it's harder to maintain a certain sort of exclusive culture. But people's temperaments differ and people

have different ways to practising law, different clientele and so on. Thus in Poland, as in Germany or France, there are still solo practices in which advocates handle practically every kind of case, as they did in the past. And when the case involves a field they don't handle, they send the client to a colleague who does and later keep an eye on how the referral work is performed.

But law firms achieve visibility today mainly by investing huge sums in advertising and promotion, generating media buzz. The media love to sell sensation, which for the legal profession is harmful. This celebrity culture has touched many law firms and many practitioners, which I find hard to square with professional ethics.

From this point of view it may be said that the development the legal profession is undergoing has good and bad sides, and how people find themselves in this world is up to them. We should remember that ultimately, who we want to be is a personal choice, a function of our upbringing, temperament, sense of decency and aesthetics, and sense of responsibility to our clients and our own family.

But won't new technologies reverse this trend, so that firms grow smaller and smaller in line with the model "a handful of lawyers plus AI"?

I believe that a large part of the practice now performed by law firms will be taken over in the future by tech firms providing automated tools and offering services directly to clients. We already see programs facilitating performance of information and opinion legal work. These are machines for drafting simple contracts and compiling responses to simple legal questions. Over time—and it seems to me rather sooner than later—they will be able to handle increasingly complex tasks. Any development stumbles over small barriers at the outset which are quickly cleared away. And when fundamental barriers are removed, progress occurs dramatically.

I believe the work of lawyers, including in law firms, will be limited to the most difficult work, with the greatest intellectual input, i.e. working directly with clients to assist them in taking decisions without stress. Specialists may be replaced by machines, but it will still be only humans who are in a position to perform creative work, where the creativity is a function of the client's complicated situation—not just legally, but also psychologically and emotionally. In performing this creative work, humans will obviously be supported by technology. Thus I believe that in a certain sense the legal profession will return to the starting point, and we will do what great lawyers and reputable firms were doing a hundred years ago.

What fosters innovation, at the level of the firm and the economy? And should we worship innovation?

First we must know what innovativeness is. Ideas come first, and innovations follow. It seems to me that until we have our principles in order, the set of values that guide our action in solving problems, which is the essence of our work, there is nothing on which to innovate. Innovations are the implementation of ideas, setting values into operation. We have to know what we're doing and why, and only after that how. Innovation is about the "how" part of know-how. There are no limitations on innovation, but we must remember that people skilled at innovation do not necessarily have the best grasp of principles.

You mean certain innovations are better not introduced?

No. Any technical solution or innovation is morally neutral. That aspect becomes relevant only when people begin applying the innovation. And obviously when an innovation is exploited by people in bad faith, it is harmful. If it is exploited by people in good faith, for worthy, socially useful aims, it is beneficial. It is not technology that is harmful, but the people wielding it.

Obviously, any invention that exerts certain changes will function for some time unnoticed. We must learn to recognise the social and cultural effects of innovations when they are introduced. The system of regulations should be aimed at eliminating the negative consequences carried by innovations. Thus, after some time it is prohibited to bring smartphones to school, just as smoking at school was banned.

Should regulations seek to prevent concentration of the power of these technologies in the hands of just a few people around the world?

This takes us back to the issue of good faith and bad faith. In his book *Building a Bridge to the 18th Century: How the Past Can Improve Our Future*, Neil Postman wrote that any technological change forces us to ask ourselves several questions: what problem is the technology supposed to solve, whose problem is it, who may be most seriously harmed by the change, what new problems may be created by the technology, and who will gain special economic and political power as a result of the change?

We must recognise that to some degree, any innovation may be used in bad faith and abused by some group to control the society or access to the advantages generated by the invention. This also raises the question of how civil society should protect against this. This is the most vital issue at the moment, as technologies have also brought about changes in systems of

democracy and the rule of law. Mechanisms invented in the 19th century and crystallised in the mid-20th century have proved dysfunctional in the collision with activity by people employing technologies in bad faith. The question is who will strike first? Citizens introducing regulations to combat abuses of technology, or groups mobilising with the express aim of subordinating these technologies to their own ends?

It's probably always the case that at the beginning no one realises the consequences that may flow from any given invention. It is only after some time that we can see more precisely how the invention can be used, for socially beneficial or harmful ends. Then the appropriate regulations must be enacted. This is the overriding obligation of lawyers in the immediate future: to understand the emerging technological processes and formulate clear rules enabling abuses to be identified and liability to be imposed for improper use of technology.

An example is bots generating fake news, sowing dysfunction in democratic systems. People realised they had been manipulated, and now we should expect countermeasures to expel this negative phenomenon from public life. Obviously another set of problems will arise when the next inventions are launched. That's why we must be vigilant at all times, observing the impact of these devices on the functioning of young people and education, while also clearly recognising the unlimited possibilities opened up by new technologies. We need to assimilate what's good and eliminate what's bad. That's all. Ultimately it all boils down to a battle between good and evil, and in this sense our world today doesn't differ at all from what it was thousands of years ago.

Tomasz Wardyński
adwokat, founding partner

Interview conducted by Justyna Zandberg-Malec

should we worship innovation?

Krzysztof Wojdyło

Legal challenges of artificial intelligence

AI systems are more and more boldly colonising our world. They are becoming an inherent element of reality, generating an urgent need to fashion rules for their functioning. It's irrelevant whether visions of AI seizing control of humans come to fruition on the foreseeable horizon. Such radical scenarios don't have to materialise for us to grasp the challenge we face. Even much more modest AI systems generate similar challenges.

Autonomy

Solutions based on AI are characterised by several properties that make it difficult to apply familiar, existing legal constructions to them. AI systems could be treated as a more advanced type of software, except that some of them have achieved a form of autonomy. This introduces a fundamental, qualitative change requiring the law to take an entirely new and original approach to such systems.

There is a certain moment, hard to define or grasp precisely, where the effect of the operation of an AI system extends beyond the scope of an intentional, intellectual causal connection between the system and its human creator. Let's consider this using the example of an algorithm that generates digital images imitating the style of artistic geniuses.

The creators of these algorithms merely created a self-learning mechanism which, after analysing enough data, is capable of identifying and imitating the unique style of a given painter. The works emerging from the virtual paintbrush of this digital algorithm are not the works of the programmers who created the self-learning algorithm. The algorithm has an autonomy about it that breaks the connection between creation of the algorithm and creation of the image. By the same principle, the creator of a tool, even one that is very intellectually refined, such as a computer processor, is not regarded as the creator of a work generated using the computer equipped with the processor.

Of course there is an unbreakable, functional, but-for causal link between the creator of the processor, the processor itself, the computer, and the works generated by the computer, but it not a connection to which we would ascribe any fundamental legal significance.

What differentiates the example of a processor from the example of an algorithm painting pictures is the lack of a human factor in the chain of dependence. Some human typically stands between the creator of the processor and the creator of the work generated by a computer using the processor, and that person is the focus of the bundle of rights connected with the work generated using the computer. In the example of the algorithm, that element is lacking. Here, there is no longer any human element between the person creating the algorithm and the work generated by the algorithm.

An algorithm is thus a tool that has itself become a creator. It has achieved the attribute of creative action. Accustomed to existing legal institutions, we could ignore this, but that would be an approach that negates reality, disregarding the change contributed by autonomous AI systems. With that approach, the law rejects a new dimension of reality and abdicates the attempt to bring legal order to it.

Entity

This autonomy of AI systems gives rise to the debate on the legal personhood of such systems. Traditionally it is the capacity for autonomous action that has been regarded as one of the fundamental attributes enabling the recognition of legal personality.

The results of the creative autonomy of algorithms may represent clear economic value. It thus becomes vital to determine which entity becomes the locus of the bundle of rights and obligations associated with the work created by the AI system.

The absence of a direct causal connection with human action means that it is not obvious at all that this bundle should be attributed to an entity recognisable under the current legal system. Even if we opted for such a solution, it would have to be determined which entity this bundle should be assigned to (the creator of the algorithm, the holder of the copyright to the algorithm, or perhaps the provider of the data enabling the algorithm to develop its own creative skill?) The current legal system cannot unequivocally resolve this doubt.

Conversely, accepting that the algorithm itself should be regarded as a new legal entity generates a number of serious practical difficulties. In this case, the algorithm would have to interact legally with other legal entities. This would be impossible in many instances. While AI algorithms may be characterised by a sort of creative autonomy, this does not necessarily extend to

making autonomous statements of will on the disposition of works generated by them. At least with respect to certain AI systems, such statements would have to be issued by traditional legal entities. In this context, the need arises for determining which entities would be entitled to issue statements of will with respect to a given algorithm.

Resolving these doubts would seem to require legislative intervention. The need for such intervention will become ever more pressing with the continued development of AI systems and the growth in value of the works autonomously generated by them. Other challenges facing the law of AI systems will also have a major impact on the ultimate shape of this determination.

Liability

The legal personality of AI systems is also tied to the problem of liability for the actions of such systems. A logical consequence of recognising that the creative autonomy of AI systems breaks the causal connection with human actions is to recognise that this connection is also broken in the context of a person's potential liability for the action of the autonomous system.

Assigning liability to a legally recognised entity for actions it had no influence over would conflict with fundamental principles of civil and criminal liability. In practice the reality might be much more nuanced. The degree of autonomy of AI systems could differ. In some cases there might be grounds for finding that an entity recognised by today's law contributed to some degree to the action of a given AI system, which would warrant at least partial liability.

It seems that in this instance as well, legislative intervention will be required. Without it, an increasingly important element of our reality, the consequences of the operation of AI systems, would suffer from systemic uncertainty.

Supervision

Another vital challenge is to establish the rules for supervision of algorithms. Generally, administrative law is used to create a framework for the autonomy of legal entities. No civilised legal system permits unlimited autonomy of action. From this perspective, the autonomy of AI systems creates a potentially dangerous gap in the system.

With this in view, we should expect attempts to introduce administrative regulations applicable to AI systems. This will not be an easy task, but presents numerous technical and organisational difficulties. Firstly, the software market would have to become a regulated industry, which conflicts with the paradigm governing its functioning so far. For many software developers, coding was

the legal personality of AI systems is also tied to the problem of their liability

and is comparable to freedom of speech. Regulating coding would be hard to accept for a large portion of the coder community.

Regulating the market would also require a system to be developed enabling specialised administrative bodies to audit algorithms and influence their action in situations where the output of algorithms' autonomy would conflict with the legal order of the state. But in some circumstances it could be difficult to audit or intervene in algorithms.

Many algorithms are created as "black boxes." The "logic" of such algorithms eludes human perception; that is, we are not always in a position to predict in advance how the algorithm will behave under given circumstances. This hinders the task of auditing such algorithms before they are launched. Returning to the example of the painting algorithm explored earlier, we cannot predict in advance whether, for example, a picture generated by the algorithm will constitute a wrongful act (e.g. because it contains pornographic elements).

In such instances, it is vital to have the possibility of administrative intervention in the operation of algorithms that are already functioning. This is relatively easy to imagine in cases where the algorithm functions as software operating in a centralised model (e.g. software installed on devices belonging to a readily identifiable entity). In such case, the competent administrative body could take certain actions against the entity in possession of the infrastructure where the algorithm is installed. A decidedly greater challenge will be to intervene in an algorithm functioning in a decentralised environment, for example as a smart contract on a public blockchain. In that case, there is no easily identifiable entity against which administrative measures could be targeted.

Human rights

The challenges described above demonstrate that notwithstanding their potential advantages, AI systems also create fundamental threats to human rights. The basic source of this threat is the autonomy of AI systems and the limited degree of control over them.

So far we have been using an example here that creates a relatively minor threat to our rights and freedoms. We can certainly imagine an algorithmic painter creating a work that infringes the dignity of specific individuals. But the impact of such an infringement would be relatively small compared to the potential negative consequences of the action of AI systems involved in decision-making processes, directly or indirectly affecting the legal situation of individuals.

Given the dynamically progressing complication of reality, it is more than certain that in taking social and economic action, we will increasingly rely on

AI systems. They are capable of much more efficiently analysing large sets of data necessary for effective administration of socioeconomic processes. Such AI systems might generate determinations addressed to specific people. In this way AI systems could directly or indirectly shape their situation. The contemporary legal system has many safety devices in place ensuring that fundamental human rights, such as dignity and non-discrimination, are taken into account when issuing decisions affecting the legal situation of individuals.

But in the case of AI systems, the criteria for taking such decisions may be subordinated to the system's autonomy. We have no guarantee that fundamental human rights will be factored into these criteria. Passivity in the face of this threat may result in the near future in our relinquishment of control over reality, at least in part, to systems for whom ensuring the individual the possibility of maximal exercise of his or her human dignity will not be an overriding aim or operating criterion.

Such situation would mean a fundamental change in the social and cultural paradigm in which we function. The contemporary legal system focuses its attention on the individual. The individual's rights are the touchstone in shaping the tools we use in our attempt to establish and conduct the socioeconomic order. If we care about maintaining this approach, we must find a way to ensure that the process of creating AI systems and the new economy based on such systems fits within the paradigm of human rights. Whether we rise to this challenge will be vitally important to our future.

Krzysztof Wojdyło
adwokat, partner in charge of the New Technologies practice

Jakub Barański
Łukasz Lasek

Cybercrime and the new paradigm of liability

> "If something can be botched, spoiled, forged, stolen, embezzled, extorted or swindled, regardless of whether such destructive behaviour pays off for the 'bad actor' or merely affords him the disinterested delight of outwitting security measures, of destroying what was valuable to another with no gain to himself, we can be absolutely certain that in new forms, new technology, the struggle between Ahriman and Ormuzd, of evil with good, will continue. Because it was always thus."
>
> Stanisław Lem, "The Risk of the Internet"[1]

Criminal cases are one of the key areas where our firm has served clients over the past 30 years. During that time the methods for fighting criminals have changed greatly. In the late 1990s common crime gave way to economic crime. It has been evident for many years now that criminality as such is moving into cyberspace. Year on year the number of traditional offences is declining, while the number of offences committed with the use of IT networks and computers is growing.

This should come as no surprise. The more personal and business matters are handled by internet, the more tempting an environment it becomes for various types of crimes. Recently traditional organised crime groups, previously involved in the drug trade and VAT fraud, have also begun to take an interest in the internet.

Fraudulent activity in cyberspace is relatively safe and cheap. Even though every operation online leaves digital traces, the solution rate for cybercrime remains very low. And it may generate a spectacular return on a small investment. Amazing IT skills are not required to carry out the business email compromise (BEC) scams that have become common in recent years, or ransomware attacks

1 "Ryzyko Internetu," essay (in Polish) collected in *Bomba megabitowa* (The Megabit Bomb) (Kraków: Wydawnictwo Literackie, 1999).

(encrypting computers and demanding ransom to decrypt them). All it takes is to purchase the right software or services online.

Cross-border cybercrime and the national justice system

The growing importance of cybercrime has not gone unnoticed by law enforcement authorities. Today nearly every country in the world has a specialised unit for combating cybercrime. For example, Poland created cybercrime units of the police and the prosecution service in late 2016 and early 2017. Europol has its European Cybercrime Centre (EC3), and in the US the FBI has its Internet Crime Complaint Center (IC3). But these are elite units used to defeat the most dangerous criminal groups. Staff and financial limitations do not allow these units to be deployed in most cases of cyber offences.

This means that on a day-to-day basis, cybercrime cases reach local police precincts, where the officers do not have adequate training or technical equipment to combat cybercrime.

Yet cybercrime, like the internet itself, most often take a cross-border form, which hinders effective action by law enforcement authorities tied down to their own jurisdiction. For example, even if the perpetrators of phishing attacks are Polish residents targeting victims within the same country, they will probably operate via servers located in Israel or South Africa, and the stolen funds will be transferred to bank accounts in China or Malaysia. Along the way they will probably use "straw men" from several more jurisdictions. A cross-border money transfer using proxy servers will take the criminals just a moment, but from the perspective of Polish law enforcement authorities it means at least several months of highly bureaucratic resort to foreign legal assistance.

Although spectacular successes in the battle with cybercrime are not unheard of, they usually involve the work of multinational teams specially formed to uncover organised crime groups at the operational level. An example is Operation Triangle,[2] carried out under the aegis of Europol and Eurojust by the Central Bureau of Investigation of the Polish National Police, along with authorities from countries like Belgium, Georgia, Italy, Spain and the UK. Rank-and-file police and prosecutors leading investigations in individual cases have little chance of identifying the perpetrators of cyber offences, not to mention apprehending them. The victims of cyber offences also cannot count on recovering their stolen funds, as the money trail in cybercrime is just as hard to trace as the perpetrators themselves. Most often cases filed with the

2 https://www.europol.europa.eu/newsroom/news/international-operation-dismantles-criminal-group-of-cyber-fraudsters

police end with detention and charges against straw men who open a bank account, take out a SIM card for a telephone, or take other auxiliary actions necessary for commission of the target offence by perpetrators parked at a computer screen in some distant country.

International corporations in the fight with cybercrime

Most cyber offences require the use of infrastructure of providers of a range of "critical services" or institutions of public trust, such as financial institutions, telecoms, and electronic services platforms.

The most common cyber offences are fairly crude in an IT sense. They are largely based on sociotechnology, i.e. techniques for manipulating people through a knowledge of psychology (a method used for example in phishing attacks, BEC frauds or the variation known as "CEO fraud"). Thus in most cases it would be more accurate to refer to "cyber-facilitated" offences. They require less financial input and skill on the part of the perpetrators than technically advanced offences (e.g. based on malware, an infected network of computers (botnets), or "zero-day exploits" targeting vulnerabilities in IT systems), but when properly done can generate equally high profits.

In frauds based on sociotechnology, use of the infrastructure of an institution of public trust allows the criminals to build credibility in the eyes of the potential victim. When an email with instructions for making a bank transfer gives a number for an account at a bank that actually exists and enjoys a recognised brand, it becomes easier to decide to transfer funds to the account. Moreover, the services provided by financial institutions or telecoms are essential to the criminals for commission of the offence for purely technical reasons. The stolen funds must be transferred into an account opened at some bank, and a bogus SMS must be sent from a number registered by a telecommunications operator.

It is precisely such supranational organisations as banks and telecoms that now find themselves on the front line in the battle with cybercrime. They have the greatest opportunity to defeat such phenomena by identifying suspicious activity before the fraud is committed. They are destined for this role both by the cross-border nature of their business, enabling activities to be coordinated across multiple jurisdictions, and by the key role of their infrastructure in commission of certain types of cyber offences.

States are more and more tightly encircling such businesses with various regulations designed to ensure the safety of their users. After all, businesses owe their commercial success to the trust of users. Thus they are required to exercise due care for users' security in areas where the state cannot reach and would not be as effective. But as is always the case in such instances, it is not

the harshness of the regulations but their enforceability that determines their effectiveness. State regulatory authorities do not have the resources at their disposal to ensure regulatory compliance. So injured parties more and more often pursue claims not against the perpetrators, who remain unidentified, but against intermediaries who failed to apply due diligence to prevent the commission of offences using their infrastructure.

Legal liability as an incentive to take action

Large international organisations like banks rarely fall victim to cyber offences themselves. They are highly aware of the dangers in cyberspace and can invest much more than the average business in building the appropriate protections. They also feel responsible for providing IT security for their customers and their deposited funds and data. But this sense of responsibility rarely extends to third parties victimised by frauds committed relying on their infrastructure and reputation.

But the position of financial institutions and other institutions of public trust is gradually changing in this regard. Banks more and more often release public warnings of various types of frauds committed under cover of electronic banking services (informational campaigns by banks warning against phishing attacks), and some telecoms publish reports on threats identified by their internal cybersecurity teams (such as reports by the Computer Emergency Response Team at Orange Polska SA). But there still cannot be said to be measures aimed at general prevention of cyber offences committed using their infrastructure. This is understandable to some extent, as unlike public authorities, providers of critical services do not bear a general obligation to combat crime. As institutions of public trust, however, they operate within an extended web of regulations providing for public-law obligations tied to some degree to combating cybercrime and crime in general. These include for example anti money laundering and counter terrorist financing (AML/CTF) obligations imposed on financial institutions, and the obligation to report breaches of personal data or data covered by telecommunications secrecy. Since the implementation of the Network and Information Security Directive, there is now an express statutory obligation to cooperate with public institutions within the national cybersecurity system.

The scope of compliance by institutions of public trust and operators of critical services with these duties largely depends on enforcement of compliance by regulators—including, in Poland, the General Inspector of Financial Information, the Personal Data Protection Office, and the Ministry of Digital Affairs. But the regulators' capabilities in this respect may be limited due to an overload of responsibilities or the lack of budgetary or staff resources.

private enforcement is a key tool for combating cybercrime

However, individual commercial actors may also enforce compliance with regulations of public law. This refers to private enforcement, the possibility for a person injured by failure to comply with public-law obligations to assert a claim against an obligated institution. In our view this is a key tool for combating cybercrime, particularly frauds of the BEC or phishing type, which piggyback on the infrastructure of banks and telecoms. The risk of liability in damages provides a strong incentive for ensuring due performance of essential obligations in this respect. The effectiveness of this mechanism is recognised by lawmakers as well, particularly at the EU level. The option for persons injured by a violation of public-law obligations to assert a private claim is already expressly provided for in EU regulations governing competition and data protection.

Private enforcement as a method for preventing cyber offences

The significance of the private enforcement mechanism is evident in the example of BEC offences. In simple terms, the fraudsters hack into correspondence (typically by email) between two regular commercial partners, pretending to be one of them. When a regular transfer of funds for contracted goods or services is expected, they instruct the unwitting victim to make the transfer to a different bank account. The account is controlled by the criminals, and was opened in advance using a straw man, who stands ready with instructions to forward the funds on to accounts opened in other jurisdictions, or withdraw it in cash and physically deliver it to his bosses. The United States and Europe suffered a wave of such offences in late 2014 and early 2015. They are relatively easy to pull off (although they require significant organisational preparations), and the potential profits are quite high. Each transfer may run to as high as a million dollars or euros, and criminals who organise an efficiently operating network of straw men need not limit themselves to a single victim.

A vital link in offences of this type is the bank. The fraudsters must open a bank account that will be under their control and enable them to pay out the proceeds. Here is where regulations imposing AML obligations come into play. If the bank scrupulously performs its obligation to identify and verify the identity of new customers, and the initial screening for money-laundering risk, often it can recognise at the stage of opening the account that the new customer is most likely operating as a straw man and is opening the account for suspicious ends, and then the bank can notify the competent institutions. It is similar with the duty to exercise ongoing oversight for money laundering and hold suspicious transactions to give the authority responsible for financial security in the given country time to act.

When due care is exercised, offences of the BEC type become much harder to carry out. Efforts to stop the wave of this type of cyber offences were largely successful due to heightened scrutiny by banks and other financial institutions. But this heightened scrutiny resulted not from warnings published by the public authorities, such as the Polish Financial Supervision Authority or the American FBI, but from concerns over the potential liability in damages to injured parties. From mid-2015 courts in Europe began to issue rulings holding that banks can be held liable in tort to third parties for violating their duties to combat money laundering.[3]

Similar cases have also been filed against some banks in Poland but have not been decided yet, and it is hard to predict how the rulings will go. The issue of the possibility of holding an institution like a bank liable in damages for infringing public-law duties, e.g. in the AML area, would be precedent-setting and entails certain serious legal problems.

Legal barriers to private enforcement in Poland and the new paradigm of liability

A basic legal barrier to holding a bank or other type of obligated financial institution liable in tort for infringement of the AML/CTF Act is the issue of how to understand the fundamental condition of unlawfulness. To find a bank's behaviour to be unlawful, is it sufficient to show that it conflicted with any obligation (command or prohibition) established by universally binding law? Or is it also necessary to show that the infringed duty was specifically aimed at protecting the very financial interests that were infringed as a result of failure to comply with the obligation? The question, in other words, is whether the bank acts unlawfully in every instance where it fails to comply with AML duties (and someone is injured as a result), or only when the duties in question were expressly aimed at protecting this category of persons against a loss.

In the proceedings conducted in Poland, the banks obviously rely on the latter conception, arguing that the AML/CTF regulations are not aimed at protecting the interests of individual participants in trade, but at protecting the safety of the financial system as such. This conception is referred to in Polish legal theory as "relative unlawfulness," and the other approach is referred to as "absolute unlawfulness." There are certain arguments of a systemic nature suggesting that Polish tort law is closer to the conception of relative unlawfulness.

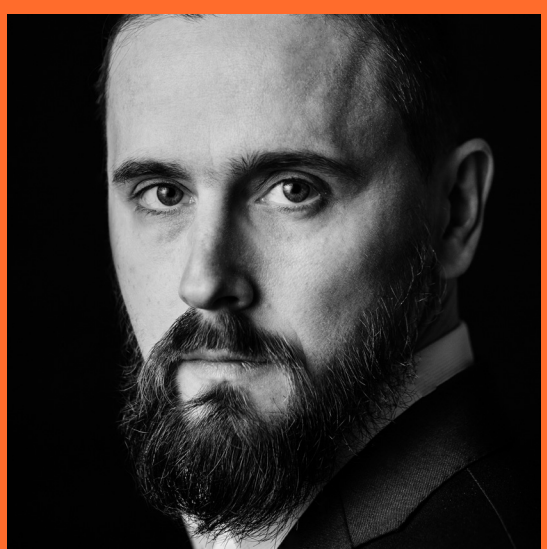
3 E.g. judgment of the Luxembourg Court of Cassation of 26 March 2015 (no. 24/2015) and judgment of the Supreme Court of the Netherlands of 27 November 2015 (no. 14/03217).

In our view, however, the key to resolving this issue is considerations of a purposive nature. For the reasons discussed earlier, enabling persons injured by cyber offences to pursue damages from the financial institutions used for this end is the only chance to raise the safety of digitalised financial dealings. It is financial institutions that have the greatest opportunity to effectively combat offences of this type. Given the scale of their operations and the progress in digitalising them, they have the best knowledge of the current threats and methods for combating them. The risk of liability in damages operates in this respect as a powerful incentive to take the appropriate steps to ensure the safety also of third parties, and not only the banks themselves and their own customers.

In cases involving banks' violation of duties to combat money laundering, the point is not so much to resolve the theoretical legal issue of the nature of the condition of unlawfulness in Polish tort law, as it is to take an entirely new look at the role of institutions of this type in the context of the contemporary digital economy. The courts must decide whether the huge scale of operation of banks and other financial institutions should also entail equally far-reaching duties of a social nature. For now we can only wait for a ruling. But regardless of the ultimate holding, the judgments issued in these cases will undoubtedly impact the scope of liability of other institutions of public trust, in other areas of law.

Jakub Barański
adwokat, Dispute Resolution & Arbitration practice

Łukasz Lasek
adwokat, Dispute Resolution & Arbitration practice, Business Crime practice
solicitor in England and Wales (not currently practising in that jurisdiction)



Sabina Famirska
Marcin Kulesza

Competition law in an age of AI and blockchain

Artificial intelligence and blockchain technologies raise new challenges for many fields of law. Both phenomena are already visible in the area of competition law. AI, in the context of algorithms, has been noted in European and global competition practice, and blockchain is an increasingly important subject of consideration.

E-commerce—algorithms and illegal arrangements

AI technologies in the form of pricing algorithms have been the focus of competition authorities and international organisations for some time.

In June 2017 the OECD published a report entitled "Algorithms and Collusion: Competition Policy in the Digital Age," devoted to an analysis of the threats to competition posed by algorithms. As pointed out in the report, the widespread use of algorithms may benefit businesses and consumers, but can also facilitate the formation and maintenance of illegal arrangements, particularly price collusion, with no formal agreement in place or even without human intervention of any kind.

In August 2016 the UK Competition and Markets Authority issued a decision on online stores operating on the Amazon platform. The CMA found that Trod Ltd and GB eye Ltd had violated the ban on anticompetitive arrangements by agreeing not to "undercut each other's prices" when selling goods via the Amazon UK site. The sites used pricing algorithms to oversee compliance with this arrangement. The CMA imposed a fine of GBP 163,371 on Trod, while GB eye took advantage of the leniency programme and avoided a fine.

In June 2018 the Luxembourg competition authority issued a decision in the case of Webtaxi, a platform for booking taxis by telephone, internet, or mobile app. When a customer placed an order for a taxi, the platform assigned the nearest taxi and set the fee in advance, based on established criteria including

a fee per kilometre, the distance, traffic conditions, and an initial fee. The price was nonnegotiable and binding on the customer and the driver. In the regulator's view, although the system did constitute a price arrangement limiting competition, it did not violate competition law. Stressing the benefits generated for both customers and businesses (reduction of travel costs, shorter waiting time for both the passenger and the driver, fewer empty vehicles), and further pointing out that the system covered only some 26% of the market and drivers still competed with one another, the regulator held that the platform qualified for an individual exemption from the ban on anticompetitive arrangements. This decision is the subject of debate, however, and the regulator's analysis of the benefits of the system is criticised.

Also in June 2018, the Russian competition authority imposed a fine on LG Electronics RUS. The authority announced that it had punished a practice involving establishment of recommended resale prices on LG's Russian website, notification to resellers, monitoring of resellers' compliance with the recommended prices, and forcing them to apply those prices, including through the use of sanctions for noncompliance (withholding supplies). This would be a classic case of vertical fixing of resale prices, were it not for the fact that LG used special software based on pricing algorithms to monitor and control the use of the recommended prices.

Then in July 2018, in four cases using a mechanism similar to the Russian LG case, the European Commission imposed fines totalling over EUR 111 million on producers of home appliances and electronics (kitchen appliances, portable computers, and audio equipment). The producers established resale prices for their products with online retailers and monitored their execution of the arrangement using special software. As in the Russian LG case, the producers of the equipment applied sanctions against non-complying retailers.

As the Commission stressed, the limitation on freedom of sellers to set prices had a broader impact on the market than just on the entities covered by the arrangement. This is because most online sellers used programming based on pricing algorithms, which automatically adjust the seller's prices to reflect competitors' prices. Thus a price increase by players covered by the schemes developed by the appliance manufacturers also impacted other retailers competing with them.

The British and Russian cases discussed above were reflected in the OECD report.

As is apparent from these examples, algorithms applied by various entities in the process of setting sale prices have a dual impact on competition. On one hand they serve as a tool for introducing and monitoring arrangements between businesses seeking to limit price competition. The risk should be noted

in this regard connected with the use of algorithms monitoring competitors' prices, which could lead to constant price coordination, excluding competition and resulting in higher prices.

On the other hand, algorithms and price-comparison tools used in monitoring competitors' prices greatly expand the negative consequences of arrangements between only a portion of the sellers on the market. The aggravated harm of vertical price arrangements, extending well beyond the circle of immediate participants in the price-fixing, significantly raises the financial risk of antitrust fines imposed on organisers and participants of such schemes.

In both respects, the use of algorithms may give rise to or increase the liability of entities involved in anticompetitive pricing practices.

In light of the foregoing examples, the summary of threats connected with the use of pricing algorithms presented in July 2018 by the German federal antitrust authority, the Bundeskartellamt, is instructive. It identifies four areas of risk. First, in sectors taking advantage of data analysis, e.g. in online sales, the use of algorithms may lead to greater transparency of the market and facilitate direct price arrangements by automation and expansion (as in the European Commission cases) of the application of prices covered by the scheme. Second, the use of algorithms in and of itself may constitute an arrangement limiting competition, without the need for direct contacts between the undertakings. Third, in self-learning systems, the algorithms may take key decisions on their own which can limit competition. Fourth, the use of algorithms may conceal price arrangements from discovery by the competition authorities, and hinder identification and prosecution in cartel cases.

Based on this analysis, far-reaching demands for changes in German competition law were formulated by the Bundeskartellamt. It was proposed to introduce a presumption that anticompetitive use of pricing algorithms leads to increased prices, and to extend liability for violating the ban on anticompetitive arrangements to cover entities such as suppliers of IT services including pricing algorithms. Similar analyses and conclusions should also be expected in other legal systems.

The topic of AI is currently the subject of sweeping work by the European Commission. Along with the member states, by the end of 2018 the Commission is supposed to develop a coordinated action plan in this area. One of the main elements of this work is to draft a code of ethics for development of AI, consistent with the Charter of Fundamental Rights of the European Union and reflecting the traditional principles guaranteeing free competition, such as transparency and data accessibility. One of the areas expected to be covered by the ethical principles is transparency of algorithms.

Blockchain and competition risks

The other major point of contact between new technologies and competition law is blockchain. This technology is growing and finding broader application. But significant competitive risks connected with its use have already been identified. The OECD also addressed this issue in its recent report.

An essential element of blockchain is the flow and exchange of information. Recording information in the chain means it is at least potentially accessible to any user. The transparency of transactional data lowers the competitiveness of the market and may lead to coordination between competitors, even coordination or fixing of prices. As in the case of pricing algorithms, blockchain could be used to conclude and monitor performance of anticompetitive arrangements.

Blockchain is closely tied to standardisation. Establishment of new standards for the purpose of compatibility of platforms must reflect the risks associated with potential restriction of users' access to platforms and the blockchain itself. Thus standards must be transparent, and access to platforms and technology must be uniform and non-discriminatory. Various blockchain platforms should be interoperative, thus ensuring transparent and easy interaction between them.

The risk of abuse of a dominant position is relevant in the context of blockchain. The technology may become essential for competing on a certain market (e.g. the quasi-financial market or using smart contracts). The entity controlling such technology may exert an influence over competition on the market. The risk of abuse may thus extend to limiting access to technology essential for counterparties and competitors to conduct business. Delay or prevention of the introduction or expansion of competing blockchain technologies by an entity dominant on a certain market connected with this technology is also a concern. A situation can be imagined where an entity controlling a certain blockchain platform reduces the cost of access to the platform, exposing it to an accusation of predatory pricing, leading to a flow of users away from competing platforms, thus excluding them from the market.

Finally, formation of a consortium with blockchain as its subject or using blockchain as a tool may constitute a concentration for purposes of competition law, giving rise to an obligation to notify the concentration to the competition authority responsible for review of concentrations.

One of the most interesting topics related to blockchain is the possibility of using this technology to solve problems involving "durable media." This issue became prominent in Poland recently in connection with decisions by the national competition authority—the president of the Office of Competition and Consumer Protection (UOKiK)—challenging the practice of several banks

providing customers access to new terms and conditions and fee schedules only via the bank's internal e-banking system. Such information is supposed to be provided to bank customers using a "durable medium." A letter in traditional or electronic form is regarded as a durable medium, as is a USB carrier or CD-ROM, and email when it contains the essential data. Providing customers access to these documents via the e-banking system was found not to meet the criteria for durability because the bank could freely modify or delete the content.

This threat may be eliminated by an appropriately developed blockchain technology recording the documents in distributed form, not allowing the content to be modified. Currently the possibility of applying this technology in dealings with consumers is being tested by one of Poland's leading banks. The position of the Polish competition authority on this issue is not yet known, but it appears that there is a high probability that under certain conditions, blockchain technology may be found to meet the criteria for a durable medium.

Consequences

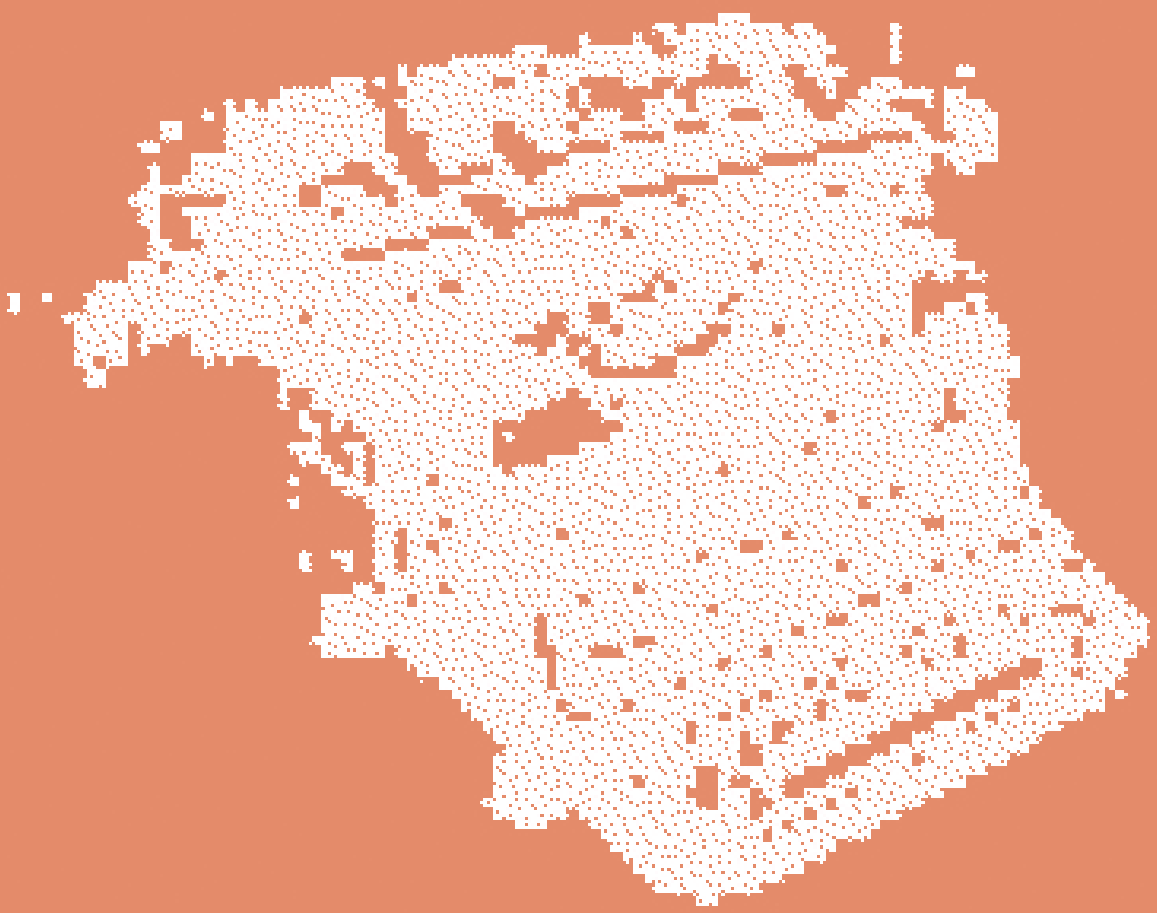
The risks of infringing competition law discussed above in connection with pricing algorithms and blockchain touch on all three of the principal areas of competition regulation: anticompetitive arrangements, abuse of a dominant position, and review of concentrations.

Each of these risks is associated with liability of the undertakings involved in the activity in question. Under Polish law, infringement of competition law in each of these areas carries the potential for imposition of a fine by the president of UOKiK of up to 10% the undertaking's annual turnover. Individual responsibility of managers for conclusion of anticompetitive arrangements by the undertaking must also be taken into account.

The higher these risks are, the lower is the certainty of compliance with the law. However, the risks may be minimised by conducting a detailed antitrust analysis of the ventures using these technologies. In particular, it is vital to consider the relevance of competition law in any instance of coordination or cooperation, in the area of programming based on algorithms for setting or monitoring prices, and technology based on blockchain.

Sabina Famirska
attorney-at-law, Competition practice

Marcin Kulesza
Competition practice



Krzysztof Wojdyło

Data: the fundamental assets of the new economy

The global economy is increasingly based on data. Data are becoming the fundamental element driving new business models. But the legal system is not prepared for this change. The future of the economy and individuals will hinge on how the law approaches data.

Data-based economy

The visible rise in importance of data in the contemporary economy is a product of several factors. First, along with the progressive digitalisation of reality, our socioeconomic system generates more and more data. Second, we have better and better tools at our disposal for processing the data we generate. Third, we have discovered the huge potential inherent in data. Appropriate processing of data generates added value, delivers new knowledge about reality, creates interesting business models, and builds competitive advantages. Fourth, data have become a fundamental resource essential for the growth of artificial intelligence systems.

The business models of companies like Google and Facebook provide an excellent illustration of the potential carried by data. Thanks to access to vast quantities of data about users, these firms could create a new model for the advertising services market. Processing data about users provides previously unencountered possibilities for profiling marketing messages. Unleashing the potential connected with data has revolutionised the marketing industry. And this is just an example of one of many business models that may arise based on data.

Who has rights to data?

More and more commonly in commerce, legal relationships are formed with data as their subject matter. Colloquially, we are beginning to refer to notions such as contracts for "sale," "lease" or "use" of data.

But there is no coherent understanding of "data" in the legal system. There are a number of isolated regulations referring to selected legal aspects of data. Probably the best-known and most recognisable example is the regulations governing personal data. They are indeed often cited as one of the fundamental factors limiting the growth of the data-based economy. These regulations define many important aspects of rules for processing of data. But they apply only to personal data. Moreover, they do not resolve key civil-law issues connected with the potential rights to data.

Data are undoubtedly becoming a new asset. This is essentially a digital asset which may be reused multiple times without being exhausted. If data are not the subject of intellectual property rights defined by the legal system, they fall into a legal vacuum. This can easily be imagined with a tangible example. Suppose there is a startup developing AI systems. The systems are fed large quantities of data collected on the company's server. The market value of the data stored on the server exceeds many times over the value of the server itself. Pursuant to execution of a judgment issued against the startup, the company's creditors take ownership of the server where the data are recorded. What rights are there to the data on the server, and who holds such rights? Did the creditor take title only to the server, or also to the data recorded on the server? If only the server, then what claim does the startup have against the creditor for the data left on the server? How to legally justify a demand to turn over possession of data, assuming that they do not constitute personal data?

Today many of these questions remain unanswered, because the legal system does not define the content of the rights to data. There is no counterpart to the right of ownership with respect to data which would enable an entity to effectively enforce its rights against anyone who infringes it. Not only that, among lawyers there is a growing dispute over whether such a right to data should be established or recognised at all.

This dispute is largely caused by a concern that introduction of the equivalent of ownership with respect to data could create dangerous limitations on trading in data. The potential of the data-based economy can only be achieved if the free flow of data and the possibility of processing data are ensured. "Ownership" of data could throw up a hurdle in this context that would be hard to clear.

On the other hand, regulation of the legal status of data is becoming an urgent need in the face of the dynamic growth in legal relationships with data as their subject matter. Without determining the civil-law meaning of the right to data, trade in this new economy will carry too big a risk.

The broader context

Defining the legal status of data will undoubtedly require intervention by lawmakers. However, the legislative solution will have to reflect the broader context of this issue. The discussion of the legal status of data doesn't have to do only with introducing a technical solution facilitating trading in data. It also means establishing the principles serving as the foundations for the data-based economy.

The essence of the decision that must be taken by the parliament largely boils down to determining the role of the individual in a data-based economy. One of the overriding values of the European legal system is the dignity of the individual. Institutions of European law strive to ensure maximum protection and realisation of this dignity.

But a data-based economy creates grave threats to the dignity of the individual. First, it creates a risk of stripping individuals of their privacy, which, at least until recently, was treated as an inherent element of human dignity. Second, it creates a risk of depriving the individual of dignity in an economic sense through a kind of "socialisation" of data generated wholly or partially by individuals.

The risk to privacy is clearly visible in the case of popular, well-known internet services that build their business models on the basis of users' data. We observe a natural tendency to force users to turn over to such services greater and greater quantities of data about their own behaviours and preferences.

The economic dimension of the risk is essentially that even though in practice individuals are often the suppliers of the raw material in the form of data, they do not participate proportionately in the benefits arising from the added value generated by processing of their data. The currently predominant model assumes that data will be provided for free, in exchange for services delivered by online suppliers. True, we can use free internet search engines or social media sites, but there are many indications that the value of the data we provide greatly exceeds the value of the benefits we access in return. This is particularly vital considering that in the face of progressive automation in the economy, which may reduce employment, we urgently need alternative methods for individuals to generate income. Data are a natural raw material which in the era of digital reality is generated by each of us by the mere fact of functioning in socioeconomic space.

Protection of individual dignity in the new economy carries a price. It is slowing down the growth of new business models, particularly solutions based on AI. Jurisdictions deciding to protect individual dignity will have to accept—at least in the short term—that they will sacrifice the leading position in the growth of the new economy.

The dilemma presented above is no doubt much more nuanced in practice. Nonetheless, it essentially presents a choice between protection of individual dignity and the effective growth of the new economy. This dilemma will be resolved in large measure on the occasion of resolving the legal status of data. What will prove crucial in this instance is a creative approach, which we hope will enable a compromise to be reached, ensuring protection of individual dignity while reaping the benefits of the data-based economy.

Krzysztof Wojdyło
adwokat, partner in charge of the New Technologies practice

About the firm

Wardyński & Partners has been a vital part of the legal community in Poland since 1988. We focus on our clients' business needs, helping them find effective and practical solutions for their most difficult legal problems.

We maintain the highest legal and business standards. We are committed to promoting the civil society and the rule of law. We participate in non-profit projects and pro bono initiatives.

Our lawyers are active members of Polish and international legal organisations, gaining access to global knowhow and developing a network of contacts with the top lawyers and law firms in the world, which our clients can also benefit from.

There are currently over 100 lawyers in the firm serving clients in Polish, English, French, German, Spanish, Russian, Czech, Italian and Korean. We have offices in Warsaw, Poznań, Wrocław and Kraków.

We share our knowledge and experience through inprinciple.pl—our portal for lawyers and businesspeople, the firm Yearbook, the new tech law blog (newtech.law), and numerous seminars, publications and reports.

wardynski.com.pl
inprinciple.pl
newtech.law

The series of publications marking the 30th anniversary of Wardyński & Partners offers a concise cross-section of texts summarising and synthesising our first 30 years of practice. Drawing from our experiences, we present visions and solutions for the future.

The second volume is focused on innovations. We discuss our manifesto explaining why lawyers must devote more attention to new technologies. Once we win the right to internet access, will the time come to recognise a right to be free from the internet? We write about how law practice has changed over the first 30 years of the firm's existence. We recall our pioneering beginnings, and address the challenges presented by the autonomy of artificial intelligence systems. We suggest how to deal with cybercrime, which can hardly occur without involving financial institutions in some way.

We examine the impact AI and blockchain have on competition law. We address the dilemma of how the law should approach data as a fundamental asset of the new economy, when the value of the data we generate greatly exceeds the value of services we receive in exchange for our data.

30yrs WARDYŃSKI & PARTNERS