GIS Odyssey Journal

2023 • Volume 3 • Number 1

https://doi.org/10.57599/gisoj.2023.3.1.149

Dorota Benduch[1]

# NEW TECHNOLOGIES IN REAL ESTATE MANAGEMENT AND PROTECTION OF PRIVACY

**Abstract:** The article examines the impact of new technologies on the property market, focusing on the integration of geospatial analytics with artificial intelligence (AI) to improve property management and gain competitive advantage. The analysis considers how AI tools, tailored to individual preferences, can assist in the management of large datasets that are critical to various sectors, including residential, commercial, office and hospitality. The primary research question addresses the extent to which the application of these innovative technological solutions affects privacy. The study identifies both challenges and potential risks, particularly in relation to privacy. It analyses the legal frameworks at national and European level, highlighting important similarities and differences. It concludes that current legal systems may struggle to adapt to the technological boom and the complexity of emerging technologies, in particular AI. The research highlights a gap in understanding the impact of advanced technologies on individual privacy and underlines the importance of responsible and ethical use of technology.

**Keywords:** Proptech, geo-spatial analysis, new technologies law, right to privacy, real estate

Received: 30 August 2023; accepted: 27 October 2023

[1] University of Economics in Katowice, Faculty of Spatial Economy and Regions in Transition, Department of Energy Transition, Katowice, Poland, ORCID ID: https://orcid.org/0000-0002-4575-7168, email: dorota.benduch@ue.katowice.pl

## Introduction

With the rapid advancement of technology, the property market has undergone a revolutionary change. Traditionally conservative and based on established management models, the market is now evolving under the influence of proptech - the innovative fusion of 'property' and 'technology'. Tools such as Artificial Intelligence (AI), the Internet of Things (IoT) and GIS systems with machine learning algorithms have fundamentally changed the way property is managed (Trincado-Munoz et al., 2023).

The use of geospatial data is central to proptech. Thanks to AI-based geospatial analysis, it is possible to accurately assess the location and potential of properties, which in turn makes it possible to predict market trends or identify building problems. Proptech also introduces the concept of smart buildings, which use the Internet of Things (IoT) to improve occupant comfort and energy efficiency. This contributes to sustainable development goals. Such innovations also support the idea of smart cities by changing the way people interact with their environment.

However, technological advances also bring challenges. While tools such as AI and IoT offer myriad benefits, their use also leads to the collection of vast amounts of data, which may violate users' privacy. This begs the question: to what extent does the use of new technologies in property management affect privacy?

To answer this question, it is essential to understand the complex relationship between technological benefits and privacy responsibilities. Key players in the property market, from managers to lawyers and regulators, need to be prepared for the challenges of modern technology.

This paper aims to analyse the impact of digital innovation and technology on the property market and assess the implications for privacy. With the increasing use of technology in property management, both lawyers and regulators need to be aware of the potential implications. As these tools become more prevalent in society, it is important to understand their ethical and legal implications.

## Materials and methods

The study focuses on the legal aspects of the use of innovative technologies in property management. Special attention is paid to the issue of protecting the privacy of its users. The article was prepared using the legal-dogmatic method, including an analysis of legal regulations, including the Constitution of the Republic of Poland (Constitution, 1997), and a literature review. A comparative method was also used, contrasting national legislation with European regulations on the right to privacy.

Considering the new legal context of technologies in property management, the research was based on contemporary national and European legislation. The focus was on constitutional provisions, private law provisions and standards under the ECHR (European Court of Human Rights, n.d.) and the GDPR (Regulation (EU) 2016/679). In addition, the Council of Europe's position on artificial intelligence (AI) was assessed, in particular with regard to the work of the Committee on Artificial Intelligence (CAI, 2023).

The aim of this study is to identify potential normative areas that could affect the rights of property users and influence subsequent decisions related to the integration of new technologies in property management. While the study is grounded in the context of Polish law, its findings may be valuable for other jurisdictions facing similar regulatory challenges.

## Results and discussion

The property market is undergoing a period of intense digital transformation, disrupting traditional business models and increasing transparency, efficiency and competition. At the heart of these changes is PropTech, a response to the demand for smart, sustainable development and economic growth. Defined as the broad application of innovative technologies in the real estate sector, PropTech offers benefits to users, property managers and land managers. It includes property selection tools, drones, virtual reality, building information modelling (BIM), data analytics, AI, IoT, blockchain, smart contracts and technologies related to real estate crowdfunding and fintech (Siniak et al., 2019). These innovations can increase productivity, improve energy efficiency and promote environmental conservation, enabling countries to make progress in line with the 2030 Agenda for Sustainable Development (UNIDO, 2016).

Technological advances have transformed real estate management over the past decade. Such tools have become indispensable and have introduced new methods of management and communication. Oxford University's concept of 'PropTech 3.0: the real estate of the future' (Baum, 2017) posits that PropTech is central to the future of property management. This now encompasses not only the property sector, but also related areas such as smart cities, the sharing economy, ConTech and FinTech. The World Economic Forum classifies the development of PropTech into three main phases: the initial development of online listing sites (PropTech 1.0), the incorporation of data analytics and virtual reality to enhance the customer experience (PropTech 2.0), and the exploration of emerging technologies such as drones, virtual reality tools, IoT and blockchain (PropTech 3.0) (Couse, 2018).

Modern property management is increasingly using tools such as geographic information systems (GIS). As a tool for collecting, storing and analysing geographic data, GIS has a core spatial analysis capability that facilitates the study of spatial patterns, affiliations and dependencies (Clapp et al., 1997). This capability, coupled with geocoding, provides property professionals with a deeper understanding of spatial relationships and paves the way for more accurate property valuations.

Geospatial analytics, especially when supported by artificial intelligence (AI)-based tools, play a central role in the transformation of the property sector. This technological amalgamation enhances the study of urban development trends and facilitates the identification of rising demand for different property genres in different locations. At the heart of this is the ability of AI-driven models to decipher a wide range of geospatial data, including aspects such as location, neighbouring infrastructure characteristics and public transport availability. Using historical price records, these models can predict future property values in different areas. One manifestation of this methodology is

Zillow's 'Zestimate' tool, which cleverly combines geospatial verification with AI to provide accurate property value estimates using a comprehensive dataset of geolocation details (Zillow, 2023). Assessing the value of a property, particularly in locations that are undergoing rapid change, requires the evaluation of numerous variables. The 'Zestimate' algorithm, which integrates deep learning methods and geospatial analytics, can take into account complicated factors such as a property's proximity to educational institutions, parks or shopping centres, in addition to a region's price history. As a result, a property's value can be meticulously assessed, taking into account not only its intrinsic attributes but also its external context.

A key area of technological intervention is the assessment of investment risk. Sophisticated AI blueprints allow property investors to meticulously assess the latent risks associated with investing in specific locations. These analyses incorporate data sets such as criminal activity, predicted climate change, natural disaster threats and expected demographic escalation. Cutting-edge AI-driven tools from leading technology companies are fusing this geospatial information from multiple sources to provide a comprehensive analysis (WeWork, 2023). In addition, AI is having a significant impact on space optimisation, as evidenced by WeWork's use of advanced sensors coupled with AI to study office space usage patterns. By monitoring employee movements on a daily basis, these systems can modify and optimise space usage, resulting in increased efficiency and comfort.

In the real estate panorama, image recognition technologies cannot be overlooked. Tools such as those presented by Orbital Insight autonomously identify property features in aerial photographs (Orbital Insight, 2023). Combined with AI-driven environmental and climate risk analysis, investors can gain a more holistic view of the potential hazards associated with specific properties, such as the risk of flooding or fire. HazardHub is an example of a platform that fuses geospatial intelligence with advanced AI paradigms to provide complex risk analysis (HazardHub, 2023).

The digital transformation of the property industry is evident in the rapid evolution of technologies such as the Internet of Things (IoT) and blockchain technology. The infusion of IoT into smart buildings fosters an interconnected web of devices and sensors, laying the foundation for smart homes. In such environments, systems facilitate the remote manipulation of functions such as heating or lighting via mobile devices (Sarah Shaharuddin et al., 2023). For property managers, IoT is emerging as an important tool, allowing them to collect and analyse data from a myriad of devices to optimise resource management and identify user preferences (Daissaouia et al., 2020). At the same time, blockchain technology is burgeoning, ensuring transparency and security of transactions, while cloud innovations enable global access to remote data.

A key tool in the property sector is BIM (Building Information Modelling). Its evolution introduces the concept of the digital twin – a virtual mirror that reflects tangible structures and processes (Sasikumar et al., 2023). This digital surrogate helps to monitor, evaluate and predict the behaviour of real-world objects, streamlining accurate management. Augmented by data analytics, cloud resources or artificial intelligence, the digital twin enables risk prediction and optimisation, which is critical for the real estate sector (Afanasjew, 2021).

In addition, these technological advances have implications for property security and preservation. Drones, also known as unmanned aerial vehicles (UAVs), are revolutionising property surveillance. They enable meticulous property assessment, area analysis and property marketing with stunning visuals (Stępień-Załucka, 2022). As well as providing accurate property valuations, drones make it easier to inspect sites for potential investments. Equipped with imaging devices, they also improve the security of properties. However, the use of drones could breach the boundaries of privacy. Similarly, surveillance mechanisms such as CCTV cameras could invade the privacy of individuals (Badowska & Badowski, 2019). With these advances comes the risk of cyber-attacks on sophisticated building management systems. Technology providers therefore have a responsibility to ensure privacy, which requires the implementation of robust safeguards (Finn & Wright, 2016).

## Right to privacy for immovable property users. A comparative analysis of national and European regulations

Modern information and communication technologies (ICT), including the Internet, are an integral part of people's daily lives. These technologies serve as central communication channels, offering convenience, speed and access to a vast reservoir of information. As a primary means of communication, the Internet is both a source of information and a threat to privacy. Inappropriate use of technology poses serious challenges. With the rapid evolution of technology, age-old privacy protection tactics are becoming obsolete. Privacy incidents are escalating, increasing the threat to the right to privacy. There are many instances where our data is collected and processed without our knowledge, leading to privacy violations.

This makes it all the more urgent to develop rules that can cope with today's technological challenges. Such rules need to be adaptable to ever-changing technologies, while ensuring robust privacy safeguards. The modern paradigm of data protection requires a fusion of reactive legal intervention and foresight in order to identify and address future dangers in advance (Petrović, 2022).

In Poland, the right to privacy occupies a fundamental position among civil rights, which is strongly supported by the Constitution of the Republic of Poland (Journal of Laws, 1997). In particular, Article 47 of the Constitution reinforces the right to privacy by stating that everyone has the right to the protection of his or her private and family life, dignity and reputation, as well as to the management of his or her personal life. This protective umbrella is further strengthened by Article 51 of the Constitution, which emphasises informational autonomy (Karpiuk, 2017).

The cited provision bifurcates and addresses two scenarios. The first concerns the individual's right to legal protection, while the second emphasises autonomy in decision-making. The first scenario emphasises the state's duty to enact formidable legal constructs that protect 'private life, family life, dignity and reputation'. The latter emphasises individual freedom, especially in the area of decision-making (Sarnecki, 2016).

In Poland, constitutional regulation has not led to a consistent definition of the right to privacy. It's synonymous with the guarantee of freedom and equality, but it's also seen as a tool to protect identity and dignity from discrimination or unjustified intrusion into the private sphere (Karpiuk, 2017; Constitutional Tribunal, 2014).

The arguments presented so far help to delineate the scope of the protection of privacy in different facets of human life. It encompasses the protection of the integrity and sanctity of this asset, as well as an individual's expectation that others won't access their private information without consent.

It follows that privacy is a staunchly defended constitutional value, and the right to privacy can be seen as a broad clause under which individuals find protection in their relations with both other individuals and the state (Uliasz, 2018). Privacy is an area that should be immune from intrusion, with individuals having the prerogative to set limits on the exposure of their personal lives. The subjective scope of the right to privacy encompasses everyone, which means that it includes both natural persons, such as Polish citizens and foreigners, and, according to the Supreme Court's rulings, legal persons in terms of honour and reputation (Supreme Court, 2008).

It's important to note that the right to privacy does not enjoy unlimited constitutional protection. Article 31(3) of the Constitution of the Republic of Poland sets out the conditions under which it may be restricted (Florczak-Wątor, 2019). However, such restrictions can only be introduced by law and are only allowed if they meet certain strict criteria, which ensure that they don't trample on the core of rights and freedoms (Karpiuk, 2015).

According to the Polish Constitution, every individual has the right to privacy and the right to defend it. As a result, privacy violations can occur in scenarios where, for example, surveillance drones interfere with the autonomy of private and family life or damage the reputation of neighbours. Importantly, it is up to the individual to determine the extent to which private family data is shared with others. In the context of drone surveillance, potential civil liability must be considered, primarily in relation to possible violations of personal property protected by the Civil Code (Civil Code, 1964). The aforementioned reference to personal property requires an explanation of this concept. In legal discourse, personal property is understood as intangible values that are relevant to the social functioning and mental state of an individual. The list in Article 23 CC isn't exhaustive, as the inclusion of a particular asset is determined by specific criteria (Olejniczak & Radwański, 2021).

At the international level, the importance of protecting privacy is underlined by instruments such as the 1948 Universal Declaration of Human Rights, the 1950 European Convention on Human Rights and the 1966 International Covenant on Civil and Political Rights. The European Court of Human Rights in Strasbourg emphasises the need to protect personal data in the age of digitalisation, taking into account communication methods such as the internet and email (Popović & Jovanović, 2017).

The right to privacy is protected internationally, particularly in the context of human rights. The European Convention on Human Rights, to which Poland is a signatory, is the central document guaranteeing this right in Europe. Article 8 of the Convention regulates this right, paragraph 1 of which states that "everyone has the right to respect for his private and family life, his home and his correspondence". This clause aims to protect the individual from arbitrary action by public officials and is largely individualistic (Kroon and Others v. the Netherlands, 1994).

The personal scope of this right extends to 'everyone', as made clear in Article 1 of the Convention, which states that 'the High Contracting Parties shall secure to every person within their jurisdiction the rights and freedoms set forth in Chapter I of the present Convention'. Legal literature points to an inaccuracy in the translation of this article. The inaccuracy is in the phrase where the High Contracting Parties guarantee rights and freedoms to 'every person'. However, legal scholars argue that the emphasis should be on "every person" and not just "the person". As a result, the right to privacy is not limited to natural persons alone, making its personal scope broader than the official translation suggests (Garlicki, 2010).

The Convention's rights and freedoms are primarily directed at natural persons, including those under the jurisdiction of the state and foreigners. It's important to understand that jurisdiction is not limited to the borders of a state, but can include acts that have effects outside its territory. Thus, the scope of jurisdiction is not limited to the geographical borders of a particular state, but can include acts that have effects outside its borders (Uliasz, 2018).

The material scope of Article 8 of the Convention includes the terms 'private life', 'family life', 'home' and 'correspondence'. These terms are inextricably linked to the issues discussed above. Although the definitions may seem clear, the case law of the ECHR reveals the complexity of their interpretation. For example, the ECHR has articulated that the scope of 'private life' is so broad that it defies exhaustive definition (Costello-Roberts v. the United Kingdom, 1993). It also encompasses facets of one's existence such as identity, both in mental and physical integrity, and includes elements such as reputation, honour and the collection and disclosure of personal data (Garlicki, 2020). At the same time, this autonomy empowers individuals to make personal choices. This autonomy extends not only to trivial choices, but to all matters of concern to the individual, including the prerogative to determine the end of one's life. The ECHR has emphasised in its judgments that this ability to decide embodies the power to direct one's life, even if it leads to decisions that may be morally or physically dangerous (Pretty v. the United Kingdom, 2002).

It follows that the right to privacy, as recognised by both the Polish Constitution and the European Convention, becomes crucial when assessing the legal implications of the use of novel technological interventions in the management of property. If such technologies interfere with an individual's daily life, they may violate Article 8 of the Convention. Thus, measures such as drone surveillance of property could fall under the protection of the ECHR.

Within the European Union, the Charter of Fundamental Rights clarifies the right to privacy, emphasising the protection of personal data (Article 8) and the preservation of private and family life (Article 7). Contemporary legislation, such as the General Data Protection Regulation (GDPR) of 2016, responds to current technological advances and emphasises the primacy of ensuring the confidentiality of personal data in an increasingly digital age (Tomić & Petrović, 2009).

A key issue concerns the use of surveillance in the context of data protection. A close analysis of RODO shows that several of its provisions directly address this concern. According to Article 2(2)(c) of RODO, its provisions do not apply when data are processed by individuals in the course of activities that are exclusively personal or domestic in nature. This means that the GDPR may not apply to property surveillance carried out for security reasons. In addition, Article 6 of the GDPR clarifies the circumstances in which data processing is considered legitimate. In this regard, the case law of the Court of Justice of the EU of 11 December 2014 emphasised that surveillance is excluded from the scope of the GDPR if it is aimed at protecting the genuine interests of the data controller (František Ryneš / Úřad, 2014).

Given these regulations and case law, the use of visual surveillance by a landowner against a neighbouring landowner will most likely fall outside the GDPR obligations. This applies in particular to monitoring aimed at safeguarding those 'legitimate interests' mentioned above. These interests include, in particular, the "protection of the property, health and life of the controller and his dependants". However, the application of such surveillance requires caution and adherence to the principles of the GDPR, with each case warranting individual consideration, taking into account both the rules governing the protection of personal data and the potential for civil claims arising from breaches of the right to privacy. This issue was discussed in the decision of the Polish Data Protection Authority of 17 July 2023, reference ZKE.440.81.2019. Consequently, it can be argued that surveillance aimed at the protection of property is consistent with the rights defined in the GDPR.

Contemporary legislation, which spans both international and national landscapes, attempts to navigate the intricacies of technological advances while upholding the rights and protections of individuals in an era overwhelmingly influenced by technology (Petrović, 2022). Privacy, a cornerstone of individual autonomy and well-being, is defended as an essential principle in contemporary societies. Such privacy enables individuals to defend themselves against unwanted intrusions into their personal sphere. Ensuring this privacy through transparent and lawful means is imperative.

## Artificial intelligence and smart homes: new challenges for privacy

Artificial Intelligence (AI) is driving transformative changes in various facets of our existence, and its impact on privacy and data management is becoming increasingly important. Many AI-based applications use data sets, a significant proportion of which process personal data, raising privacy concerns. The integration of AI into property management frameworks, such as smart home systems, offers users the luxury of remote device control. However, this also increases the risk of privacy breaches. Such systems facilitate remote monitoring of myriad household functions, creating new privacy and security dilemmas. AI innovations exacerbate existing vulnerabilities by facilitating extensive surveillance based on biometric or genetic data. A study by Fránik & Čermák (2020) identified critical security vulnerabilities in smart home hubs marketed by three major European companies. These vulnerabilities threaten fundamental human rights, including the right to life, liberty and security (Fránik & Čermák, 2020).

Modern technologies, especially those related to smart homes, offer countless benefits. However, they also pose risks to people's privacy and security. Security vulnerabilities in smart home devices can affect fundamental human rights such as life and liberty. Threats such as man-in-the-middle attacks, which disrupt device communication, and denial-of-service attacks can disable devices, putting users' health and livelihoods at risk.

A publication by the European Union Cyber Security Agency (ENISA) highlights the dangers of relinquishing control over devices such as thermostats or smart locks, and stresses that such vulnerabilities can directly endanger human lives. Attacks on smart homes can take many forms, from malfunctioning devices and data theft to burglary and property theft. Given the paramount importance of human safety, it is imperative to mitigate these potential threats (ENISA, 2023).

Beyond the realm of tangible security, the gravity of privacy concerns escalates, especially when considering smart homes. Cyber adversaries have the ability to monitor users and potentially access confidential information, culminating in identity theft or unwarranted location monitoring. These looming threats are multifaceted, encompassing both privacy and security breaches.

The responsibility for ensuring security lies with both manufacturers and users. Manufacturers should prioritise high security standards in their products, while users need to be aware of potential risks and exercise caution in their purchasing decisions. UNESCO emphasises the primacy of human safety when it comes to products or services that use artificial intelligence (UNESCO, 2023). The safety integrity of AI-based systems depends on their accuracy, reliability and resilience to vulnerabilities.

To address these challenges, the effective application of privacy principles in AI remains essential. The European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG) has developed ethical guidelines that highlight the importance of respecting privacy, maintaining data quality and integrity, and ensuring controlled access (AI HLEG, 2019). However, some research suggests that not all systems are impeccably secure. A study by Denko highlighted privacy vulnerabilities in certain smart home IoT devices (Denko, 2017), while another study by Apthorpe et al. highlighted the potential threat of data breaches (Apthorpe et al., 2017).

The Information Commissioner's Office (ICO) has highlighted the need to implement optimal levels of security in AI systems to prevent unauthorised or unlawful processing and to mitigate the risk of data loss, erasure or damage (ICO, 2020). In the field of AI, where myriad entities contribute to the development and operation of systems, the delineation of responsibilities becomes complicated (AI HLEG, 2019). The 2018

Montreal Declaration makes clear that humans cannot escape responsibility for decisions made by AI systems. However, it notes that holding individuals accountable for a properly functioning AI system is not justified. The OECD's definition of accountability emphasises the commitment of organisations and individuals to ensure the consistent performance of AI systems, taking into account their respective roles and the relevant legal context (AI HLEG, 2019).

Existing regulatory tools are critical to ensuring accountability for actions dictated by AI. The complexity of unravelling how algorithms work, and the apparent gaps in accountability, are becoming increasingly prominent issues. The European Parliament highlighted in its 2020 resolution that while adapting to new technologies is paramount, it doesn't require a complete overhaul of existing accountability structures (Montreal Declaration for Responsible Development, 2018). A key aspect is the recognition of humans as the primary architects and overseers of AI systems. The Parliament also advocated for changes to the Product Liability Directive to adapt it to the dynamics of modern digital technologies (Buitena et al, 2023).

In order to skilfully mitigate the adversities and repercussions of artificial intelligence, a fusion of different regulatory positions is essential. Liability paradigms can be divided into different taxonomies, including fault-based liability, strict liability and contractual liability. These categories address different objectives, particularly in terms of protecting the rights of consumers and individuals affected by AI-driven actions.

However, grappling with the nuances of liability isn't the only conundrum arising from the technological advancement of AI. A prominent feature of current AI systems is their reliance on massive datasets, which are central to the competent training and validation of AI designs. This reliance triggers profound considerations about data ownership and accessibility, which are intimately linked to the prevailing distribution scheme of economic goods. As a significant proportion of these datasets contain personal data, any misuse can potentially violate privacy.

## Conclusions

Technological advances in property management, particularly through geospatial analytics and artificial intelligence, are creating new opportunities for the property sector. This digital shift facilitates the effective processing of large amounts of data, which is becoming increasingly important in various market sectors, from residential to hospitality. Accurate analysis of this data can greatly accelerate the identification of trends and the forecasting of market shifts.

The analyses carried out highlight the potential for AI to be tailored to individual user preferences in the property sector. The use of such tools is revolutionising traditional ways of working, while paving the way for new avenues of growth. The privacy implications of AI are particularly important in the property management sector. Potential privacy concerns associated with the implementation of AI in smart homes and similar technologies have been addressed in previous sections.

A predominant challenge posed by contemporary technologies revolves around the protection of privacy. The legal aspects of this concern have been addressed in the light of different regulatory frameworks at national, EU and international levels. The juxtaposition of these different privacy policies reveals both marked differences and parallels. Despite these differences, it's clear that the existing legal architecture may be ill-equipped to deal with the complexities introduced by modern technology, particularly AI.

It's clear that, despite the myriad benefits of the digital metamorphosis, there is an imperative to deeply understand the implications of such changes for individual privacy. This places a responsibility on technologists, professionals and policymakers to use technology wisely and ethically, and underlines the need for a more appropriate legal framework.

Ongoing studies exploring the impact of AI technologies on property management are recommended. The findings from the primary research question point to the urgency of continued observation and scrutiny of this rapidly evolving field. Such academic endeavours can provide invaluable perspectives that will enable the sector to skilfully navigate the evolving technological terrain while maintaining strict privacy standards.

In essence, the digital evolution of real estate is both a treasure trove of opportunities and a cauldron of challenges. The sector must be prepared to be nimble and ensure that technology is used to enhance, rather than hinder, human endeavour.

## References

Act of 23 April 1964 – Civil Code (Journal of Laws of 2023, item 1610 with amendments).

Afanasjew S. (2021). 5 steps to digital transformation in real estate. Objects, vol. 1, no. 1, pp. 14–19.

AI HLEG. (2019). Ethical guidelines for trustworthy artificial intelligence. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 [access: 01.10.2023].

Apthorpe N. J., Reisman D., Feamster N. (2017). A smart home is not a castle: Privacy vulnerabilities of encrypted IoT traffic. ArXiv. https://doi.org/10.48550/arXiv.1705.06805 .

Badowska A., Badowski M. (2019). Visual recording of real property vs right to privacy. In: IBasista, PCichociński, E. Dębińska, Gajos-Gržetić M. (ed.), 26th Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2019". Conference Proceedings, pp. 7–11.

Baum A. (2017). PropTech 3.0: the future of Real Estate. University of Oxford Research. www.sbs.oxford.edu [access: 01.10.2023].

Buitena M., de Streel A., Peitz M. (2023). The law and economics of AI liability. Computer Law & Security Review, vol. 48, https://doi.org/10.1016/j.clsr.2023.105794.

Clapp J.M., Rodriguez M., Thrall G. (1997). How GIS Can Put Urban Economic Analysis on the Map. Journal of Housing Economics, vol. 6, no. 4, pp. 368–386.

Committee on Artificial Intelligence (CAI). (2023). Council of Europe. https://www.coe.int/en/web/artificial-intelligence/cai [access: 01.10.2023].

Constitution of the Republic of Poland (Journal of Laws of 1997, No. 78, item 483, with amendments).

Constitutional Court. (2014). Judgment of 30.07.2014, K 23/11. Official Journal [Journal of Laws] 2014, no. 1055.

Couse, A. (2018, January 24). How drones, data and AI are changing the property sector. World Economic Forum. https://www.weforum.org/agenda/2018/01/proptech-drones-data-ai-property-sector/ [access: 01.10.2023].

Daissaouia A., Boulmakoulc A., Karimd L., Lbatha A. (2020). IoT and Big Data Analytics for Smart Buildings: A Survey. Procedia Computer Science, pp. 170, 161–168.

Denko M.W. (2017). A privacy vulnerability in smart home IoT devices. University of Michigan-Dearborn. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/139706/49698122_ECE_699_Masters_Thesis_Denko_Michael.pdf [access: 01 October 2023].

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (Council of Europe). https://www.echr.coe.int/documents/convention_eng.pdf [access: 01.10.2023).

European Court of Human Rights. (1993). Costello-Roberts v. The United Kingdom (Application no. 13134/87). Judgment of 25 March 1993. A.247-C, para. 36.

European Court of Human Rights. (1994). Kroon and Others v. Netherlands (No. 18535/91), Judgment of 27 October 1994. Council of Europe. https://www.refworld.org/cases,ECHR,584a99574.html [access: 01.10.2023].

European Union Cyber Security Agency [ENISA]. (2023). Security resilience good practices. https://www.enisa.europa.eu/publications/security-resilience-good-practices [access: 01.10.2023].

Finn R. L., Wright D. (2016). Privacy, data protection and ethics for civil drone practice. Computer Law & Security Review, pp. 32, 577–586.

Florczak-Wątor M. (2019). Commentary on Article 47 of the Constitution of the Republic of Poland. In: P. Tuleja (ed.), The Constitution of the Republic of Poland. Commentary. Wolters Kluwer, pp. 169–170).

Fránik M., Čermák M. (2020). Serious flaws found in many smart home hubs: is your device among them? WeLiveSecurity. https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/ [access: 01.10.2023].

František Ryneš / Úřad. (2014). C-212/13.

Garlicki L. (2010). Commentary to Art. 1 ECHR. In: L. Garlicki (ed.), Convention for the Protection of Human Rights and Fundamental Freedoms, vol. I, C.H. Beck, pp. 1–18, 34, 493.

HazardHub. (2023). HazardHub Platform. https://www.guidewire.com/products/hazardhub/ [access: 01.10.2023].

ICO. (2020). Guidance on Artificial Intelligence and Data Protection. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ [access: 01.10.2023].

Karpiuk M. (2015). Right to privacy in the conditions of new technologies. In: K. Chałubińska-Jentkiewicz, M. Karpiuk (ed.), New technologies law. Selected issues. Wolters Kluwer, pp. 321–322.

Karpiuk M. (2017). Constitutional right to privacy and its limitation due to state security. The example of secret information. In: K. Chałubińska-Jentkiewicz, K. Kakarenko, M. Wyrzykowski (ed.), Security and Freedom. Wolters Kluwer, pp. 102–103).

Kim J., Kang D. (2019). AI application in real estate: Focusing on prediction accuracy and uncertainty to enhance investment decision-making. Automation in Construction, pp. 104, 102–114.

Korohodova L., Matias M. (2019). Smart homes and private life. Cybersecurity, vol. 3, no. 4, pp. 328–334.

Lam K.C., Lim B.T.H. (1999). The use of GIS in real estate: Current applications and future directions. Journal of Property Finance, vol. 10, no. 4, pp. 382–399.

Nevelsteen K.L.J. (2017). The Grinns Tale: A prototype urban analysis tool. Cities, vol. 69, pp. 26–34.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 May 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 [access: 01.10.2023].

Polish Data Protection Authority's decision of 17 July 2020, reference ZKE.440.81.2019. https://uodo.gov.pl/decyzje/ZKE.440.81.2019 (access: 01 October 2023).

Saavedra J.R., Belda R.S. (2018). Automated Machine Learning: Review of the state-of-the-art challenges and opportunities. ArXiv. https://arxiv.org/pdf/1812.10406.pdf [access: 01.10.2023].

Sadowski J. (2019). Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives and Taking Over the World. MIT Press.

Smith L. (2021). The Real Estate Implications of Smart Home Devices. Journal of Property Management, vol. 83, no. 2, pp. 5–12.

Supreme Court. (2008). Judgment of 17 July 2008, II CSK 111/08.

The Guardian. (2019, August 9). Amazon workers can hear users' Alexa recordings, report says. https://www.theguardian.com/technology/2019/apr/11/amazon-workers-can-listen-to-users-alexa-recordings [access: 01.10.2023].

Trincado-Munoz F., van Meeteren M., Rubin T.H., Vorley T. (2023). Digital transformation in the world city networks' advanced producer services complex: A technology space analysis. Geoforum. https://doi.org/10.1016/j.geoforum.2023.103721

Van Weyenbergh J., Podoynitsyna K. (2019). Business models for sustainable innovation: State-of-the-art and steps towards a research agenda. Journal of Cleaner Production, vol. 208, pp. 841–853.

Wang L., Alexander B. (2019). How IoT changes urbanism: An analysis based on case studies. Journal of Smart Cities, vol. 3, no. 1, pp. 29–38.

Wells D., Figueiredo J. (2018). Incorporating GIS into real estate research: The benefits and challenges. The Journal of Real Estate Finance and Economics, vol. 57, no. 1, pp. 54–86.

Yurukoglu A., Corts K.S. (2020). Measuring the Benefits of Home Ownership: A Spatial Approach. Review of Economics and Statistics, vol. 102, no. 3, pp. 549–562.

Zalnieriute M., Milanovic M. (2019). The ECtHR's surveillance jurisprudence and the right to data privacy in the digital era. Computer Law & Security Review, vol. 35(5), no. 105356.