



DIGITAL MARKETING AND CYBERSECURITY IN HEALTH TOURISM: A COMPARATIVE ANALYSIS OF SPA AND HEALTH RESORTS IN CROATIA AND SLOVENIA

Patricija Kajić Kudelić, PhD Student

Ministry of the Interior

Ulica grada Vukovara 33, 10000 Zagreb, Croatia

pkkudelic@gmail.com

Nikica Milić, PhD Student

Pliva Croatia d.o.o.

Prilaz baruna Filipovića 25, 10000 Zagreb, Croatia

milic.nikica@gmail.com

Lucija Živković, PhD Student, Teaching Assistant

Josip Juraj Strossmayer University of Osijek, Faculty of Law

Stjepana Radića 13, 31000 Osijek, Croatia

lzivkovic@pravos.hr

ABSTRACT

Health tourism is one of the most dynamic segments of the contemporary tourism industry, particularly within the European Union, where the free movement of patients and the availability of cross-border healthcare services drive growing demand for specialised health tourism offerings. In this environment, digital marketing has become a key instrument for the international positioning of healthcare institutions, while the ongoing digitalisation of business processes simultaneously generates increasing requirements for cybersecurity and the protection of personal and health-related data.

* The authors disclose the use of ChatGPT and Google translate exclusively as auxiliary linguistic tools for translating limited excerpts and ensuring terminological consistency. These tools were not used for generating substantive content, legal analysis or conclusions, all of which remain the sole responsibility of the authors.

Spa and health resorts constitute a core segment of health tourism in Croatia and Slovenia, drawing on natural healing resources, medical expertise, and a long-standing tradition of rehabilitation and disease prevention. To remain competitive in the European market, these institutions are increasingly utilising digital communication and sales channels, including official websites, social media platforms, and online booking systems, in which data security is an integral component of their digital presence. This paper aims to analyse and compare how spa and health resorts in Croatia and Slovenia integrate digital marketing and cybersecurity into their business and communication practices. Particular emphasis is placed on the role of cybersecurity in digital advertising, online booking processes, and data management, as well as on its visibility in public communication directed at service users. Methodologically, the paper is based on an analysis of relevant European Union legal and regulatory frameworks, including NIS 2, the Cybersecurity Act, the Cyber Solidarity Act, and the Cyber Resilience Act, as well as a comparative case study of selected spas and health resorts in Croatia and Slovenia. The empirical component of the research includes a qualitative analysis of official websites and digital communication channels, as well as a survey focusing on managerial and marketing practices within these institutions. The results of the comparative analysis indicate that Croatian and Slovenian health resorts have a well-developed, functional digital presence, including official websites, online booking and payment, and active use of social networks. The main similarities concern the recognition of digital channels as a means of information dissemination, promotion, and building user trust. The main differences concern the intensity of content publishing, the dynamics of paid advertising, and the extent of multilingual website adaptation.

An empirical preliminary study conducted on a sample of health resorts in Croatia and Slovenia found that digital marketing is perceived as an important factor for international visibility, while cybersecurity is mainly viewed as an integral part of responsible digital business, rather than as an obstacle to digital advertising. The results indicate a high number of official websites, extensive use of digital advertising and social networks, but also limited adoption of advanced digital solutions and insufficient employee education. The main challenges are the protection of sensitive data, regulatory compliance, developing a security culture, and the high costs of investing in cybersecurity.

The paper offers both theoretical and practical contributions to the discussion of the importance of cybersecurity as a fundamental element of the sustainable and competitive development of health tourism within the European context.

Keywords: Cybersecurity, Digital transformation, Digital marketing, EU regulatory framework, Health tourism

1. INTRODUCTION

Health tourism is increasingly emerging as one of the most important specialised forms of tourism. Its significance stems from the integration of health, rehabilitation, preventive, and tourism services into a comprehensive offer aimed at maintaining and improving users' health. The development of health tourism in Europe is further driven by increasing patient mobility, greater accessibility of health services, and growing demand for high-quality and affordable healthcare-related tourism. Within health tourism, health resorts stand out as an important segment

in both the Republic of Croatia and the Republic of Slovenia. Health resorts are based on natural healing factors, which constituted the origins of health tourism, medical and rehabilitation services, and a long tradition of preventive and therapeutic treatment. Although both countries, Croatia and Slovenia, possess natural and institutional prerequisites for the development of this form of tourism, there are still differences between them, primarily with regard to the level of market profiling. Digital transformation has significantly influenced the way health tourism providers operate and communicate. In particular, online reservation systems, online payment systems, and digital communication tools such as official websites, social media, and digital marketing have led to increased market visibility, more effective communication with users, and greater service availability. At the same time, the increased use of digital processes has further highlighted the importance of information system security and data protection, particularly in sectors that process highly sensitive personal and health-related data. Cybersecurity has therefore emerged as a critical issue in modern data management within health tourism sector. Therefore, the importance of cybersecurity is not limited solely to the technical protection of information systems; it also encompasses protecting the confidentiality, integrity, and availability of data, preserving business continuity, and the mitigation of legal and other risks. This paper analyses the integration of digital marketing and cybersecurity within the health tourism sector, with a special focus on health resorts in Croatia and Slovenia. The paper aims to analyse and compare how health resorts in these countries incorporate digital marketing and cybersecurity into their business and communication practices. The paper is based on an analysis of relevant European and national cybersecurity legal frameworks, and a qualitative assessment of the digital presence of selected health resorts. Furthermore, a preliminary study was conducted with a convenience sample of employees from Croatian and Slovenian health resorts who held management, marketing, IT, or related positions. The paper is structured into six sections. Following the introduction, the second section outlines the concept of health tourism and the characteristics of its development in Croatia and Slovenia, with a special focus on health resorts as an important segment thereof. The third section provides an overview of cybersecurity through general concepts and definitions, describes the European network of legal acts through the most important documents of the European Union, and analyses and compares the Croatian and Slovenian national cybersecurity systems. The fourth section addresses digital marketing in health tourism and provides a qualitative analysis of the digital presence of selected health resorts. The fifth section presents the results of the survey on the integration of digital marketing and cybersecurity in health resorts, outlines the research limitations, and offers recommendations for future research. The sixth section presents the concluding remarks.

2. THEORETICAL DEFINITION OF HEALTH TOURISM

Health tourism is one of the oldest forms of tourism, yet it remains one of the most dynamic segments of the tourism industry. Its development is particularly emphasised in the context of the European Union, where the free movement of patients and the availability of cross-border healthcare services stimulate demand for specialised health tourism offerings. Health tourism can be divided into three main segments: medical tourism, spa tourism, and wellness tourism. Medical tourism focuses on invasive and non-invasive medical procedures; spa tourism is based on the use of natural healing factors such as thermal waters, medicinal mud, and favourable climatic conditions, while wellness tourism encompasses activities aimed at maintaining and improving health through recreation, balanced nutrition, and relaxation.¹ For destinations, health tourism extends the tourism season year-round and attracts guests with higher purchasing power, thereby serving as an important factor in economic development and in strengthening international competitiveness. Geić points out that health tourism involves staying outside one's place of permanent residence for the purpose of treatment and health improvement through the use of natural healing factors and medical procedures.² After the theoretical definition of health tourism, the following analysis examines the position and development of health resorts in the Republic of Croatia and the Republic of Slovenia as important components of the overall health tourism offer.

2.1. Comparative Characteristics of the Development of Health Resorts in Croatia and Slovenia

Among the various forms of health tourism, health resorts stand out as a particularly traditional and recognisable segment of this sector. Health resorts represent an important component of health tourism in the Republic of Croatia and the Republic of Slovenia. Their development is based on the use of natural healing resources, together with the gradual expansion of services towards medical and rehabilitative care. In these countries, health resorts constitute an important segment of the overall health tourism offer. Although both countries use natural resources for healthcare purposes, there are certain differences in the organisation of services, market orientation, level of investment, and strategic approach to developing this segment. The Republic of Croatia has significant comparative advantages in developing health tourism: high-quality healthcare services, qualified medical staff, destination safety,

¹ Smith, M., *et al.*, *Balkan Wellbeing and Health tourism study*, 2016, Available at: [BalkanWellbeingFINALREPORT.pdf], Accessed 19 March 2026.

² Geić, S., *Menadžment selektivnih oblika turizma*, Sveučilišni studijski centar za stručne studije u Splitu, Split, 2011, pp. 81-83.

competitive prices, and an abundance of natural healing resources. Health resorts are particularly prominent as specialised institutions that use thermal and mineral waters, medicinal mud, and climatic conditions for prevention, treatment, and rehabilitation under professional medical supervision. Telišman-Košuta and Marušić emphasise that the key success factors of Croatia include its favourable geographical position, good transport accessibility, membership in the European Union, high levels of safety, service quality combined with a good price-to-quality ratio, and well-preserved natural resources.³ Despite its considerable potential, Croatia has yet to fully capitalise the opportunities for developing health tourism. One of the main reasons is the strong focus on seasonal coastal tourism, which means that health tourism and health resorts are still not sufficiently integrated into the year-round development model of the tourism offer.

Unlike Croatia, the Republic of Slovenia has developed a more systematic and internationally recognised model of health tourism, particularly in the health and wellness segments. Slovenia relies on a long tradition, developed infrastructure, and stronger integration of health and tourism services. A key competitive advantage for Slovenia lies in its rich natural healing resources, particularly thermal and mineral waters, which underpin the development of numerous health resorts. Recently, Slovenia has been further profiled as a sustainable and green destination, emphasising a healthy lifestyle, prevention, and a holistic approach to health. The Republic of Slovenia has been implementing a green environment policy since 2022, with an implementation plan extending to 2028, aiming to achieve added value with a smaller ecological footprint.⁴ The focus is on energy efficiency, the renovation of medical capacities, and the expansion of accommodation capacity.⁵ Furthermore, the development of health resorts and wellness tourism in Slovenia has been accompanied by stable investment cycles aimed at modernising infrastructure, digitalising business operations, and using renewable energy sources. Such an approach contributes to strengthening the competitiveness of Slovenian health resorts and their market positioning. From a comparative perspective, Croatia and Slovenia share a similar resource base for developing health tourism but differ in the degree of integration of healthcare and tourism services, the level of market positioning, investment dynamics, and the strategic approach to

³ Telišman-Košuta, N.; Marušić, Z.. *Percepcija Hrvatske kao destinacije zdravstvenog turizma na tržištu posrednika – kvalitativno istraživanje, Konačni izvještaj*, 2018, Available at: [https://www.htz.hr/sites/default/files/2019-07/Zdravstveni%20turizam_Percepcija%20Hrvatske_Konacni%20izvjestaj_23042018_FIN.pdf2018], Accessed 19 March 2026.

⁴ Slovenian Tourism Strategy 2022–2028, May 2022, Available at: [https://www.gov.si/assets/ministrstva/MGTS/Dokumenti/DTUR/Strategija-slovenskega-turizma-20222028-/SLOVENIAN-TOURISM-STRATEGY-2022-2028-v2.pdf], Accessed 18 March 2026.

⁵ *Ibid.*

development. While Croatia possesses significant natural and professional potential, it still needs stronger integration between the healthcare and tourism sectors, whereas the Slovenian model appears to be more systematic and internationally recognised. It is precisely these similarities and differences that provide an important framework for the further analysis of digital presence and the integration of digital marketing and cybersecurity into the business operations of health resorts.

3. ASPECTS OF CYBERSECURITY

Cybersecurity has become an indispensable part of the economy, development, defence, and other important segments of society. Cyberattacks, due to their unpredictability, their potential to cause significant damage, and their ability to spread rapidly across national borders, represent a major priority for the European Union (EU) and its Member States. Today, cybersecurity encompasses everything from cybercrime to state-sponsored attacks. The rapid advancement of technologies and the sophistication of attack methods continue to pose significant challenges.⁶ The concept of cybersecurity should be understood as extending far beyond a merely technical issue. This area plays a crucial role in promoting economic stability, enhancing investment attractiveness, and fostering innovation potential.⁷

3.1. Concept and Meaning of Cybersecurity

Cybersecurity is one of the most significant challenges of the 21st century. Conceptually and theoretically, it can be observed as part of information security and national security, and it is certainly closely related to the protection of critical infrastructure. The interweaving of different domains, such as political, social, economic, and security domains, such as defence, demonstrates the complexity and demanding nature of this field. The costs of cybersecurity⁸, as well as the costs of security breaches, are increasing globally.⁹ Companies need to allocate significant resources in order to cope with cybersecurity risks; additionally, to remain competitive, they must keep pace with rapid technological change through

⁶ Svete, U., *Cybersecurity between technological determinism, political governance and national security challenges*, Journal of Comparative Politics, Vol. 2, No. 2, 2025, p. 108.

⁷ Ravlić, S.; Unukić, I., *Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: Institucionalne i geopolitičke perspektive*, Festung: časopis za interdisciplinarna istraživanja u poslovanju, No. 2, 2025, p. 143.

⁸ ConCERT conference held in February 2026 showed that the costs of damage caused by cyberattacks are increasing. In addition to official data, it is clear that the real figures are more significant, since a part of cyberattacks are never reported and therefore not included in official statistics.

⁹ Saeed, S. et al., *Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations*, Sensors, Vol. 23, No. 15, article no. 6666, 2023, p. 2.

continuous investment.¹⁰ To understand any field, particularly one as complex as cybersecurity, clear definitions of key concepts are essential to ensure a shared and consistent understanding. There are no universally accepted definitions of cybersecurity or related concepts¹¹, and differences in definitions can be found both in legal acts and in scientific and professional literature.¹² The NIS 2 Directive¹³ provides definitions of several terms, some of which are defined by referring to other legal acts.¹⁴ For example, cybersecurity and cyber threats are defined by reference to Regulation (EU) 2019/881.¹⁵ According to that legal act, cybersecurity encompasses all activities necessary for protection against cyber threats affecting network and information systems, their users, and other persons affected by them. In contrast, a cyber threat denotes any possible circumstance, event, or action that could damage, disrupt, or otherwise adversely affect network and information systems, their users, and other persons. The NIS 2 Directive defines an incident as an event that threatens the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or services offered by or accessible through network and information systems.¹⁶

3.2. EU Cybersecurity Legal Framework

The fundamental EU document in the field of cybersecurity is Directive EU 2022/2555 (NIS 2 Directive) of 14 December 2022.¹⁷ Significant organisational and functional differences in the implementation of cybersecurity solutions have been identified among Member States. The Directive aims to establish minimum

¹⁰ *Ibid.*, pp. 10-11.

¹¹ O debate, A. T.; Benkhelifa, E., *A comparative study of national cyber security strategies of ten nations*, 2023, [https://doi.org/10.48550/arXiv.2303.13938], Accessed 12 March 2026.

¹² Florido-Benitez, L., *The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review*, Discover Computing, Vol. 28, No. 1, 2025, p. 4.

Using the example of the definition of the notion cybersecurity, the author showed how attitudes can be different through as many as 27 more or less different definitions of one and the same term.

¹³ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80.

¹⁴ The same way of defining is used in Law on Cybersecurity (Zakon o kibernetičkoj sigurnosti), Official Gazette, No. 14/2024.

¹⁵ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L151/15.

¹⁶ Directive (EU) 2022/2555, note 14.

¹⁷ *Ibid.*

standards for cybersecurity capabilities and coordination across the entire EU.¹⁸ The Directive expands its scope and coverage, thus increasing the number of entities or sectors, which are divided into key and important sectors, namely sectors of high criticality and other critical sectors. The health sector is explicitly designated as a key sector, i.e. a sector of high criticality. Member States can no longer independently determine entities, as harmonised criteria have been introduced to ensure consistency across national systems. Particular emphasis has been placed on the need for cooperation and data exchange. In order to achieve this, obligations regarding the designation of competent authorities and rules governing their work and cooperation have been established; at the same time, the EU has established additional bodies and organisations.¹⁹ Deadlines and obligations for notifying competent authorities and reporting cyber threats or incidents are clearly defined. Furthermore, risk assessment and risk management constitute central elements of the cybersecurity framework, aimed at ensuring business continuity and minimising the adverse effects of incidents on service users and other services. Substantial penalties in cases of non-compliance and supervisory obligations within clearly defined deadlines have been established, without leaving such decisions to the discretion of Member States. In addition, the obligation to develop a comprehensive national strategy and the need to raise awareness of the importance of cybersecurity are prescribed. Based on the NIS 2 Directive, the EU Member States have further harmonised their cybersecurity frameworks by establishing minimum requirements for the functioning of a coordinated regulatory system across Member States.²⁰ The deadline for transposition of the NIS 2 Directive into national legislation was 17 October 2024.

In addition to the NIS 2 Directive, there are several other acts regulating this area, such as the Cyber Resilience Act of 23 October 2024 as Regulation (EU) 2024/2847²¹, which emphasises that cybersecurity is one of the key challenges facing the EU, with far-reaching implications for the economy, democracy, security, and public health. The EU addresses these challenges by increasing resilience. The Act defines conditions for the development of secure products with digital elements, ensuring that hardware and software products with fewer vulnerabilities are brought to the market and that manufacturers assume responsibility for

¹⁸ Svete, *op. cit.*, note 7, p. 117.

¹⁹ For example, Network EU-CyCLONe, Network of national CSIRTs, Cooperation group etc.

²⁰ Council Recommendation (EU) 2025/C 3445 of 6 June 2025 on an EU blueprint for cyber crisis management, OJ C 2025/3445.

²¹ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) 2024 OJ L327/15.

cybersecurity throughout the entire product lifecycle, including the design, development and production. Prior to this act, there was no horizontal regulatory framework in the EU establishing comprehensive cybersecurity requirements for products with digital elements. With the aim of building cybersecurity capabilities for skills development, and enabling a faster detection of cyber threats and incidents and a more rapid response, Regulation (EU) 2025/38 of 19 December 2024, known as the Solidarity Act, was adopted.²² It defines the need to establish a European cybersecurity alert system. The CSIRT system, as envisaged by the NIS 2 Directive, is an information exchange system, whereas the European alert system envisaged here is intended to represent a new capability that complements the CSIRT system. Member States retain primary responsibility for prevention, preparedness, response, and assistance, which is provided through the promotion of solidarity among Member States and the availability of technical assistance in situations of significant cyber incidents.

In addition, the EU legal framework also includes Regulation (EU) 2019/881 of 17 April 2019 on ENISA – the Cybersecurity Act. This act establishes ENISA – the European Union Agency for Cybersecurity – as a centre of expertise. The Agency has several objectives, including promoting cooperation, contributing to the strengthening of capabilities and capacity building, promoting awareness, education, research, and innovation, contributing to the development and implementation of EU policies and law, fostering international cooperation, and others.

EU activities in the field of cybersecurity should also be briefly considered in connection with recent developments on the geopolitical scene. The EU's efforts to create conditions for digital independence are increasingly coming to the forefront. The normative framework of the EU is particularly strong; however, to create conditions suitable for strengthening technological sovereignty, investments in domestic technologies and infrastructure are also required.²³ The plan for the digital decade also includes reducing dependence on other regions when it comes to key digital capacities.²⁴

²² Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 on measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) [2025] OJ L38/1.

²³ Lider, Europe searching for digital freedom, Available at: [<https://lidermedia.hr/zeleno-i-digitalno/digitalna-sloboda-europa-trazi-izlaz-iz-zamke-tehnoloskih-divova/>]. Published 18 May 2025. Accessed 04 March 2026.

²⁴ Digital future for Europe, European Council, Available at: [<https://www.consilium.europa.eu/hr/policies/digital-transition/>], Last change 11 November 2025. Accessed 04 March 2026.

3.3. Cybersecurity in the Health Sector

The health sector is defined in the EU legal framework as a sector of high criticality, while tourism is not explicitly mentioned. Health resorts combine these two areas. Cybersecurity in the health tourism sector includes protecting sensitive and confidential patient or user data, business processes, business continuity, and digital and other infrastructure. The impact of cyberattacks, that is, their consequences, may be significant and include, among other things, extortion, blackmail, and the sale of data on the dark web and other platforms.²⁵ The European Action Plan on the cybersecurity of hospitals and healthcare providers of 15 January 2025²⁶ is a response to the urgency of the situation and the unique threats facing the health sector. The issue of ensuring cybersecurity is extremely complex, and the solution is seen in prevention, detection of cyber threats, response to attacks, and recovery therefrom. Digital transformation in the health sector and its interconnection with other sectors further increase the importance of cybersecurity. The health sector is regularly targeted by cyberattacks by individuals and groups, as well as by state-sponsored campaigns.²⁷ Improving the digital skills of healthcare professionals, as well as enhancing healthcare information structure in response to the growing application of new and complex technologies in medicine and healthcare, represents an important component of addressing cybersecurity challenges.²⁸ The importance of employee education also arises from the fact that, within the cybersecurity triad of people, processes, and technology, the human factor has proven to be the weakest link. Research shows that employee actions are responsible for the majority of cybersecurity incidents.²⁹ In general, and especially in the health sector, it is necessary to ensure at least a basic level of cyber hygiene and to foster a strong culture of cybersecurity.³⁰ ENISA has issued the document Cyber Hygiene

²⁵ Alarfaj, K. A.; Rahman, M. H., *The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix*, Applied Sciences, Vol. 14, No. 13, 2024, p. 4.

²⁶ European action plan on the cybersecurity of hospitals and healthcare providers, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Directorate-General for Health and Food Safety, Available at: [https://health.ec.europa.eu/publications/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en/], COM(2025) 10 final, Brussels, 15 January 2025.

²⁷ Belani, H. *et al.*, *SWOT analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske*, Bilten Hrvatskog društva za medicinsku informatiku, Vol. 28, No. 1, 2022, p. 2.

²⁸ *Ibid.*, p. 5.

²⁹ Šolić, K. *et al.*, *Comparative Study on Online Security Awareness and Behavior Among Healthcare Professionals in Croatia*, 2024 47th MIPRO ICT and Electronics Convention, IEEE, 2024, p. 1803, [<https://ieeexplore.ieee.org/abstract/document/10569325>], Accessed 11 March 2026.

³⁰ European action plan on the cybersecurity of hospitals and healthcare providers, note 28.

in the Health Sector,³¹ which contains guidelines with simple and implementable measures for protection. The aim is to help all types of healthcare entities reduce cyber risks and strengthen their resilience.

According to ENISA data from 2023, the health sector reported the highest number of security incidents in the software or hardware vulnerabilities segment. The same source states that ransomware accounted for 54% of all analysed cyber incidents in the health sector during 2021-2023. Of these incidents, 83% were financially motivated, while 10% were ideologically motivated. According to the Commission's 2024 report, 71% of attacks affecting patient care were ransomware-type attacks. Ransomware is often combined with the leakage of patient data.³²

Additionally, according to Eurobarometer data, in 2024, only 25% of surveyed companies in the field of healthcare, education and social protection provided training or implemented awareness-raising activities related to cybersecurity. Human error remains the largest contributor to cyber incidents in the health sector, further strengthening the argument for the importance of education and cybersecurity awareness.³³ The same source states that the largest share of companies using external providers for cybersecurity tasks comes from the healthcare, education, and social protection domains, accounting for 57% of surveyed companies. In 2024, an estimated shortage of about 299,000 qualified cybersecurity experts in the EU was reported.³⁴

The health sector is among the most frequently targeted and most vulnerable sectors, according to recent data. Sensitive patient data is one reason this sector is particularly attractive to ransomware attacks. Data protection is crucial for safeguarding confidential and sensitive data and ensuring data integrity, given the ethical, legal, and health-related consequences.³⁵ Cybersecurity in the health sector should primarily ensure protection against data loss or theft, disruption of business processes, financial losses, and physical damage to infrastructure.³⁶

³¹ ENISA document with recommendations for cyber hygiene in health sector, Available at: [<https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber%20Hygiene%20in%20the%20Health%20Sector.pdf>], Accessed 04 March 2026.

³² European action plan on the cybersecurity of hospitals and healthcare providers, p. 3, note 28.

³³ *Ibid.*

³⁴ *Ibid.*

³⁵ Anson, A. *et al.*, *Ransomware attacks on healthcare systems: Case studies and mitigation strategies*, 2023, [https://www.researchgate.net/publication/376514138_Ransomware_Attacks_on_Healthcare_Systems_Case_Studies_and_Mitigation_Strategies], Accessed 11 March 2026.

³⁶ *Ibid.*

3.4. Croatian and Slovenian Cybersecurity Systems

As Member States of the European Union, the Republic of Croatia and the Republic of Slovenia have transposed the NIS 2 Directive into their respective national legal frameworks and share a common foundation for establishing cybersecurity at the national level. Croatia adopted the Cybersecurity Act³⁷, which entered into force on 15 February 2024³⁸, while Slovenia transposed the NIS 2 Directive through its act on information security³⁹, which entered into force on 19 June 2025. In Croatia, the National Cybersecurity Strategy from 2015⁴⁰ remains in force, while in Slovenia, the Cybersecurity Strategy of the Republic of Slovenia from 2016 is in force.⁴¹ The comparison of the Croatian and Slovenian systems is based on two fundamental documents, the law and the strategy. Croatia transposed the NIS 2 Directive among the first EU member states, while the Slovenian law entered into force eight months after the deadline set by the Directive. Although both states share the same goals deriving from the Directive, they have adopted different solutions in establishing their systems. Croatia regulated only the field of cybersecurity through its law, whereas Slovenia adopted a law regulating information security, with cybersecurity as part of that field. Consequently, Slovenian provisions include, for example, provisions on security checks for employees or job candidates, as well as provisions on specific characteristics of working hours in this field. Such provisions do not exist in Croatian legislation, since this area is regulated by other laws and bylaws. Although Slovenian regulations more frequently link cybersecurity to national security⁴², the law does not place the central national authority within the security and intelligence system, as in the Croatian model. Croatia has placed its National Cybersecurity Centre within the

³⁷ Cybersecurity Act (Zakon o kibernetičkoj sigurnosti), Official Gazette, No. 14/2024.

³⁸ In addition to the Cybersecurity Act (Zakon o kibernetičkoj sigurnosti), Croatia also adopted Regulation on Cybersecurity (Uredba o kibernetičkoj sigurnosti), Official Gazette, No. 135/2024, which entered into force 30 November 2024 and also Decision on the adoption of the National Cybercrisis Management Program (Odluka o donošenju Nacionalnog programa upravljanja kibernetičkim krizama), dated 09 January 2025 [<https://ncsc.hr/hr/nacionalni-program-upravljanja-kibernetickim-krizama>], Accessed 11 March 2026.

³⁹ Information Security Act (Zakon o informacijski varnosti), Official Gazette of the Republic of Slovenia, No. 40/25.

⁴⁰ National Cybersecurity Strategy (Nacionalna strategija kibernetičke sigurnosti), Official Gazette, No. 108/2015 entered into force 7 October 2015.

⁴¹ Cybersecurity Strategy of the Republic of Slovenia (Strategija kibernetičke varnosti), Available at: [https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf], Accessed 11 March 2026, entered into force February 2016.

⁴² In the Slovenian strategy, the concept of national security is mentioned through the document in a total of eight places. For the first time already in the very introduction on the first page of the strategy, when it states how cybersecurity has become an important and integral part of national security.

Security and Intelligence Agency, which is certainly one of the key institutions of the national security system.⁴³ By contrast, the competent national authority in Slovenia is the Government Office for Information Security. The Slovenian intelligence and security agency retains competence in specific segments; it does not serve as the central authority within the cybersecurity system.

Both laws divide the entities to which they apply into key and important entities, that is, sectors of high criticality and other critical sectors. The Croatian law, in addition to those specified in the NIS 2 Directive, includes the education system in the second group, while the Slovenian law additionally includes local self-government within public administration in the same category. These two states are among the few EU Member States that have adopted only one national cybersecurity strategy to date.⁴⁴ Following the adoption of the NIS 2 Directive and the corresponding national laws, neither state has changed its strategy or adopted a new one. Both strategies, as strategic documents, were adopted at approximately the same time and set out their respective goals and corresponding measures. The Slovenian strategy provides an overview of the situation at the time of its adoption, a review of risks, a system scheme, and a SWOT analysis. The Croatian strategy does not contain these elements but instead, it sets out, for example, guiding principles, and is complemented by an Action Plan for implementation, adopted to facilitate the systematic monitoring of the Strategy's implementation.

In addition to comparisons of systems based on legal regulations, the literature also contains analyses grounded in the assessment of the state of cybersecurity itself. One approach to analysing the state of cybersecurity includes three indicators: level of penetration (LP), level of digitalisation (DL), and the Global Cybersecurity Index (GCI). The GCI represents the sum of five elements: legal, technical, organisational, capacity development, and cooperation.⁴⁵ According to research conducted in 2024, eight EU Member States are considered to have below-average GCI results, and nineteen have above-average scores. Slovenia is in the former group, and Croatia is in the latter.⁴⁶ Although the Croatian strategy is characterised by fewer goals, it has nevertheless achieved above-average GCI results.⁴⁷ In addition, there is another significant difference between the two systems, namely

⁴³ Security and Intelligence System Act (Zakon o sigurno-obavještajnom sustavu) Official Gazette No. 79/2006, 105/2006 entered into force 16 August 2006.

⁴⁴ Fujs, D.; Bernik, I., *Analyzing cybersecurity of the European Union: Challenges and Opportunities for Public Administration*, Elektrotehniški vestnik, Vol. 91, No. 1–2, 2024, p. 12.

⁴⁵ *Ibid.*, p. 10.

⁴⁶ *Ibid.*, pp. 11–12.

⁴⁷ *Ibid.*, p. 12.

the SK@UT system.⁴⁸ Some states, as part of their infrastructure, use sensors designed for the fast and efficient detection of cyberattacks; Croatia is one of these states. The SK@UT system, implemented in 2019, is a national system for detecting cyber threats and safeguarding cybersecurity. It comprises a network of sensors that monitor traffic and detect anomalies and potential threats in real time. This system is recognised as one of the three leading solutions in the EU.⁴⁹

There are numerous examples of attacks on the health sector.⁵⁰ Probably the best-known attack on the health sector in Croatia occurred in June 2024 at KBC Rebro. Open sources made it possible to follow the entire incident, which served as an additional incentive to raise awareness of the importance of this segment and to implement the legal framework of the NIS 2 Directive more timely and effectively.⁵¹ One example of an attack on the health sector in Slovenia is a ransomware attack that in 2019 affected the information system of Lekarna Ljubljana. As a result of the attack, the electronic systems of around 60 pharmacies in the Ljubljana area ceased functioning, and for a period, medicines were dispensed solely on paper prescriptions.⁵²

⁴⁸ Official website of the National Centre for Cybersecurity about SK@ut system, Available at: [<https://ncsc.hr/hr/skaut>]. Accessed 04 March 2026.

⁴⁹ Svete, *op. cit.*, note 7, pp. 112-113.

⁵⁰ Although they do not apply nor to Slovenia or Croatia, let us mention some other examples of cyberattacks.

EU documents mention an example of an attack on Vastaamo. It is a Finnish company that provided a psychotherapy service and was attacked by a ransomware attack. The result of the attack was the theft of patient data, but also extortion. The attack took place in 2018, but was not discovered until 2020. Source European action plan on the cybersecurity of hospitals and healthcare providers, note 28.

Let us also mention the cyberattack which is believed to be the first cyberattack on a healthcare system that resulted in the death of a patient. Synnovis is a healthcare institution that was the victim of a ransomware cyberattack in June 2024. The cyberattack resulted in the delay or cancellation of its services and affected over 11,000 different scheduled medical procedures. Some of the stolen confidential and sensitive data was made public during the same month. In addition to the above, the cyberattack is believed to have resulted in the death of one of the patients. Source, Available at:

[<https://www.england.nhs.uk/synnovis-cyber-incident/>], Accessed 11 March 2026 and [<https://www.hipaajournal.com/patient-death-linked-to-ransomware-attack/>], Accessed 04 March 2026.

⁵¹ Information about the cyberattack on KBC Zagreb, Available at: [<https://www.dnevno.hr/vijesti/soa-se-oglasila-o-kibernetickom-napadu-na-kbc-zagreb-isticemo-i-jos-jednu-vaznu-stvar-2466699/>], Accessed 17 February 2026.

⁵² Information about the cyberattack on Slovenian pharmacies, Available at: [<https://net.hr/danas/svijet/hakeri-napali-slovenske-ljekarne-pao-centralni-informaticki-sustav-pacijenti-otezano-do-lijekova-a8c672a6-b9f2-11ec-a54f-0242ac130011?amp=1>], Accessed 11 March 2026.

4. DIGITAL MARKETING IN HEALTH TOURISM

Digital marketing most commonly includes tools such as official websites, social media, email, and digital advertising. Biloš et al. state that digital marketing encompasses the use of digital technologies, Internet platforms, and online communication channels to plan, implement, and optimise marketing activities, with particular emphasis on user interaction, content personalisation, and the measurement of communication effectiveness in the digital environment.⁵³ Saputra argues that integrating digital marketing creates opportunities for more precise market targeting, improved customer engagement, and the optimisation of the user experience. At the same time, its implementation may be hindered by technical limitations, changes in organisational culture, and a lack of understanding of digital technologies. Therefore, the successful integration of digital marketing requires investment in organisational resources, support from top management, and the development of data-driven decision-making.⁵⁴ In the field of healthcare, digital marketing assumes additional importance because it is not limited to an institution's market positioning but it also involves providing information that may influence health literacy and patients' decisions. Bavrka and Bošnjak emphasise that digital marketing in healthcare entails the integration of online strategies for the promotion of medical services and the provision of information to patients. Despite its advantages, digital marketing in healthcare requires careful handling of personal data in order to ensure patient security and trust.⁵⁵ In the context of health tourism, digital marketing has an even broader function, as it relates not only to the promotion of healthcare services but also to the presentation of the destination, accommodation, additional amenities, and the overall stay experience. Cristóbal-Fransi et al. stress that an online presence is essential for tourism stakeholders and that health resorts represent an important resource for building the image of wellness and health tourism destinations. This suggests that the digital presence of health tourism destinations is not merely a technical issue of online visibility but also a matter of competitiveness, reputation, and market positioning.⁵⁶ Furthermore, official websites represent an important tool of digital marketing in health tourism. They provide users with access to basic information

⁵³ Biloš, A.; Turkalj, D.; Kelić, I., *Micro-moments of user experience: An approach to understanding online user intentions and behavior*, CroDiM: International Journal of Marketing Science, Vol. 1, No. 1, 2018, pp. 57-67.

⁵⁴ Saputra, A., *The Importance of Digital Marketing Integration in Strategic Management Planning*, Action Research Literate, Vol. 8, No. 5, May 2024.

⁵⁵ Bavrka, T.; Bošnjak, D., *Uloga digitalnog marketinga u promociji zdravstvenih usluga*, SKEI – Međunarodni interdisciplinarni časopis / International Interdisciplinary Journal, Vol. 5, No. 1, May 2024, pp. 101-111.

⁵⁶ Cristóbal-Fransi, E. et al., *The challenge of digital marketing in health tourism: the case of Spanish health resorts*, Qualitative and Quantity, 2023.

about the institution, service types, therapies, wellness and medical facilities, accommodation capacity, location, pricing, and online booking options. Websites are also key instruments in the design of digital communication campaigns.⁵⁷ In addition to websites, social media also play an important role, enabling health tourism providers to communicate directly with users. John et al. note that social media in health tourism are most commonly used for disseminating information and interacting with online audiences.⁵⁸ Smith and Wallace emphasise that social media have become a key communication tool in the promotion of health resort services. They are regarded as one of the most important marketing strategies for increasing user loyalty.⁵⁹ Their value is particularly evident in their capacity for regular content publishing, presenting benefits and services, sharing visual materials, and creating an impression of accessibility. Kaur and Kumar further emphasise that, despite certain limitations associated with the use of social media in health resort marketing, their advantages outweigh the identified disadvantages.⁶⁰ An additional dimension of digital communication is represented by digital advertising. Elrod and Fortenberry state that digital advertising involves the paid use of mass media to deliver messages to a target audience and represents one of the most common and effective ways of engaging both existing and potential patients. Although due to a traditionally conservative approach, digital advertising in the health sector has developed more slowly than in other industries, it is now firmly established and widely used in healthcare organisations worldwide. Its importance lies in the ability to target messages precisely, segment audiences, and measure campaign effectiveness, which makes it a particularly relevant tool for health tourism as well, where competition is strong, and user decisions often depend on the quality and persuasiveness of digital presentation.⁶¹

4.1. Comparative Analysis of the Digital Presence of Terme Tuhelj and Terme Olimia

Digital channels such as official websites, social media, and digital advertising in health tourism are gaining importance; therefore, an analysis of the online pres-

⁵⁷ Marine-Roig, E. et al., *Measuring gastronomic image online*, International Journal of Environmental Research and Public Health, Vol. 16, No. 23, 2019.

⁵⁸ John, S.; Larke, R.; Kilgour, M., *Applications of social media for medical tourism marketing: an empirical analysis*, Anatolia, Vol. 29, No. 4, 2018, pp. 553–565.

⁵⁹ Smith, M.; Wallace, M., *An Analysis of Key Issues in Spa Management: Viewpoints from International Industry Professionals*, International Journal of Spa and Wellness, Vol. 2, No. 3, 2019, pp. 119–134.

⁶⁰ Kaur, K.; Kumar, P., *Social Media: A Blessing or a Curse? Voice of Owners in the Beauty and Wellness Industry*, The TQM Journal, Vol. 34, No. 5, 2022, pp. 1039–1056.

⁶¹ Elrod, J. K.; Fortenberry, J. L. Jr., *Advertising in Health and Medicine: Using Mass Media to Communicate with Patients*, BMC Health Services Research, Vol. 20, 2020, article no. 818, pp. 1–8.

ence of service providers is crucial for understanding communication with users. For the purposes of this paper, a comparative analysis of the digital presence of Terme Tuhelj and Terme Olimia was conducted, as they represent Croatian and Slovenian health resorts. Table 1 contains the basic elements of online presence, such as the functionality of official websites, presence and frequency on social media and paid advertising.

Table 1: Comparative analysis of the digital presence of Terme Tuhelj (Croatia) and Terme Olimia (Slovenia)

Element of analysis	Terme Tuhelj (Croatia)	Terme Olimia (Slovenia)
Official website	Yes	Yes
Multilingual website	HR, ENG, SLO, DEU, ITA, PYC	HR, ENG, SLO, DEU, SRP, ITA, PYC
Online reservation system	Yes	Yes
Online payment for services	Yes	Yes
Facebook presence	Yes	Yes
Instagram presence	Yes	Yes
Use of paid advertising	Yes (continuous)	Yes (seasonal)

Social media posting frequency High Moderate to high

Source: Compiled by the author, based on an analysis of the official websites of Terme Tuhelj and Terme Olimia, their official profiles on social media, and the Meta Ads Library platform

The comparative analysis shows that both institutions have a well-developed digital presence. Terme Tuhelj and Terme Olimia have their own official websites, online booking is enabled, as well as online payment. Both institutions actively use social media, specifically Facebook and Instagram. Despite the similarities, there are also certain differences. Terme Tuhelj continuously uses paid digital advertising, while Terme Olimia is characterised by a seasonal approach to advertising. The above indicates a different marketing dynamic, as well as adjustments to promotional activities during periods of increased demand. The differences are also visible in the multilingualism of the official websites. Terme Olimia offers a greater number of languages, which indicates a stronger focus on the international market. Also, differences are visible in the frequency of posting on social media. Terme Tuhelj is more active than Terme Olimia. These results indicate that both spas recognise the importance of social media for communicating with users, but approach them with different intensity. In conclusion, digital presence does not only represent an additional promotional advantage but also becomes an important factor in competitiveness and availability of services, and can influence the building of trust among users.

5. INTEGRATION OF DIGITAL MARKETING AND CYBERSECURITY IN HEALTH RESORTS

5.1. Research Methodology

The research was conducted from February 1 to March 15, 2026, using a structured online questionnaire created in Google Forms. The questionnaire was designed specifically for the purposes of this study and was based on the established research objectives as well as the theoretical and regulatory frameworks governing digital marketing, data protection, and cybersecurity in health tourism. The questionnaire consists of 20 questions organised into four thematic sections. The first section covers digital marketing in the spa business, the second cybersecurity and data protection, the third the integration of digital marketing and cybersecurity, and the fourth covers the challenges and perspectives of their integration in the spa business. Closed-ended questions, multiple-choice questions, five-point Likert-scale items, and one open-ended question were used.

When presenting the research results, more precisely, when displaying certain graphs, the number of responses may vary because three questionnaire items were optional. These questions concerned the assessment of the connection between cybersecurity and digital advertising, and priorities for future development. The above questions are not necessarily equally applicable to all respondents, given the diversity of respondents' professional roles within the institutions. Therefore, the results of the above questions were analysed and interpreted based on the number of valid responses, more precisely, on 11 respondents, whereas all other results were based on the total convenience sample of 13 respondents.

Content validity of the questionnaire was ensured by aligning the questionnaire items with the research objectives and the key concepts discussed in the theoretical part of the paper, while a check for clarity and terminological consistency was carried out before distribution. Since this is an exploratory study conducted on a smaller convenience sample and the questionnaire is not based on standardised multi-item measurement scales, formal reliability testing, such as the calculation of Cronbach's alpha coefficient, was not performed. This limitation was taken into account when interpreting the results, which should be regarded as preliminary and exploratory. The average time required to complete the questionnaire was approximately 10 minutes. The collected data were analysed using descriptive statistical methods.

The population framework of the study was formed based on publicly available sources and official websites of health tourism institutions in Croatia⁶² and Slove-

⁶² Katalog projekata zdravstvenog turizma Ministarstva zdravstva Republike Hrvatske, Uprave za zdravstvenu zaštitu, Available at:

nia⁶³. According to the National Programme - Action Plan for the Development of Health Tourism, 24 relevant health institutions were identified in Croatia, including special hospitals for medical rehabilitation, health resorts and spas, while the official list of Slovenian thermal spas and health institutions included 14 entities. A convenience sampling approach was employed in the study. Respondents were purposively selected through a review of the official websites of the selected health resorts and spas and by identifying publicly available contact details of individuals in management, marketing, IT and related positions, who were assumed to possess relevant knowledge of digital marketing, data protection and cybersecurity. A total of 23 institutions were contacted, including 11 in Croatia and 12 in Slovenia. Institutions were contacted primarily by email, and to a lesser extent by telephone, whereby due to the limited telephone response rate, further communication was conducted predominantly by email.

The sample included a total of 13 respondents from health spas in Croatia and Slovenia, with 61.5% of respondents coming from Croatian and 38.5% from Slovenian institutions. Given the use of the convenience sampling method and the limited number of responses, the results of the study should be interpreted as preliminary and exploratory, without the possibility of generalisation to the entire population of health tourism institutions in Croatia and Slovenia.

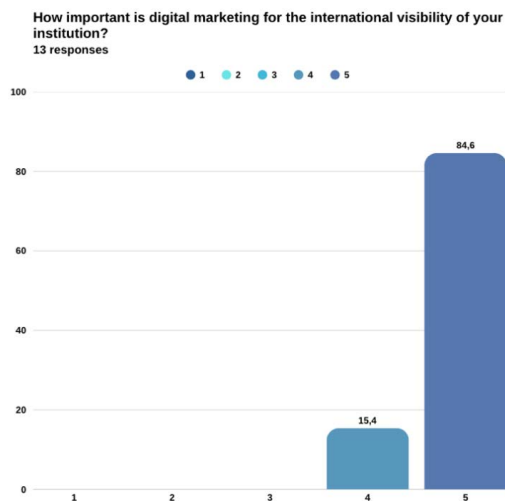
5.2. Results of the Preliminary Research

By type of institution, the most represented are medical and rehabilitation health resorts, followed by wellness and spa health resorts, thermal health resorts, and combined institutions. The results show that all observed health resorts use official websites (100%) as the primary channel of digital communication. Digital advertising (84.6%) and social networks (76.9%) are also highly represented. This confirms the dominant role of digital communication tools in the promotion of services. E-mail marketing is used by 61.5% of institutions, which indicates a relatively significant presence of direct digital communication with users. Specialised health tourism platforms are used to a lesser extent (30.8%), while virtual reality (VR), augmented reality (AR), and other forms of promotion are only marginally represented (7.7%). Health resorts continue to rely on conventional digital channels, while the application of more technologically advanced tools, such as artificial intelligence, is still limited.

[https://zdravlje.gov.hr/UserDocsImages/2025_Objave/Katalog%20projekata%20zdravstvenog%20turizma%202024.pdf], Accessed 03 June 2026.

⁶³ All thermal spas and health resorts, Available at: [<https://slovenia-spa.si/all-thermal-spas-and-health-resorts-list>], Accessed 03 June 2026.

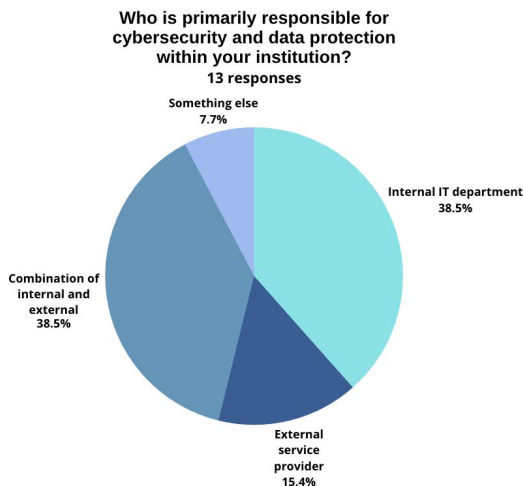
Chart 1: Assessment of the importance of digital marketing for the international visibility of the institution



Source: Compiled by the author

The results presented in Chart 1 show that the majority of respondents (84.6%) rate digital marketing as extremely important, while the remaining (15.4%) rate it as important. Given that no respondent chose lower ratings, it can be concluded that there is a clear consensus among the observed institutions on the strategic role of digital marketing in strengthening international recognition.

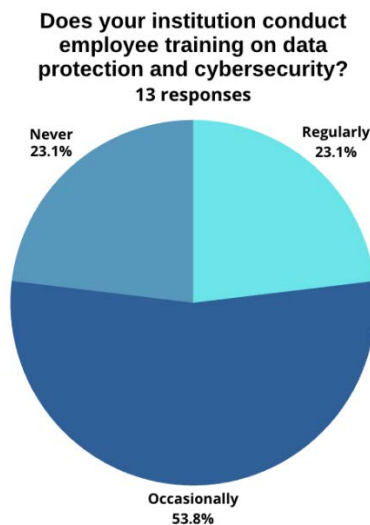
Chart 2: Primary responsibility for cybersecurity and data protection issues in the institution



Source: Compiled by the author.

The results shown in Chart 2 indicate a split model of managing security functions. In 38.5% of institutions, the internal IT department is primarily responsible, while an equal share of respondents indicates a combined model. In 15.4% of cases, security functions are entrusted to external providers, while 7.7% of respondents indicate a different organisational model. Given the results of the analysis, a hybrid approach to cybersecurity management is evident, as institutions combine internal capacities and external professional support, with the assumption of more efficient management of security risks.

Chart 3: Implementation of employee training on data protection and cybersecurity

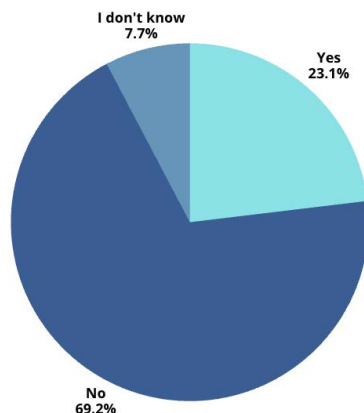


Source: Compiled by the author.

Chart 3 shows that employee training on data protection and cybersecurity at the observed health resorts is relatively low. Training is provided regularly in only 23.1% of facilities, while 53.8% of respondents report that it is provided occasionally. An additional 23.1% of respondents state that training is not provided at all in their facility. The results show that, despite the existence of formal data protection procedures, continuous training remains insufficiently systematically integrated.

Chart 4: Experience of health resorts with cyberattacks in the past five years

Has your health resort experienced
any type of cyberattack in the past
five years?
13 responses

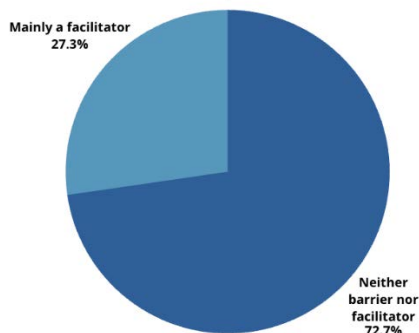


Source: Compiled by the author.

Regarding cyberattacks, 69.2% of respondents report that their institution has not experienced any during the last five years. In contrast, 23.1% of respondents indicated that their institution has been exposed to a cyberattack, while 7.7% are unsure whether an attack has even been recorded at their institution, as shown in Chart 4. The results show that although most institutions have not reported cyberattacks, cybersecurity risks should not be underestimated within the health tourism sector. Therefore, it is necessary to educate employees and develop appropriate organisational mechanisms.

Chart 5: Perception of cybersecurity as a barrier or a facilitator in digital advertising

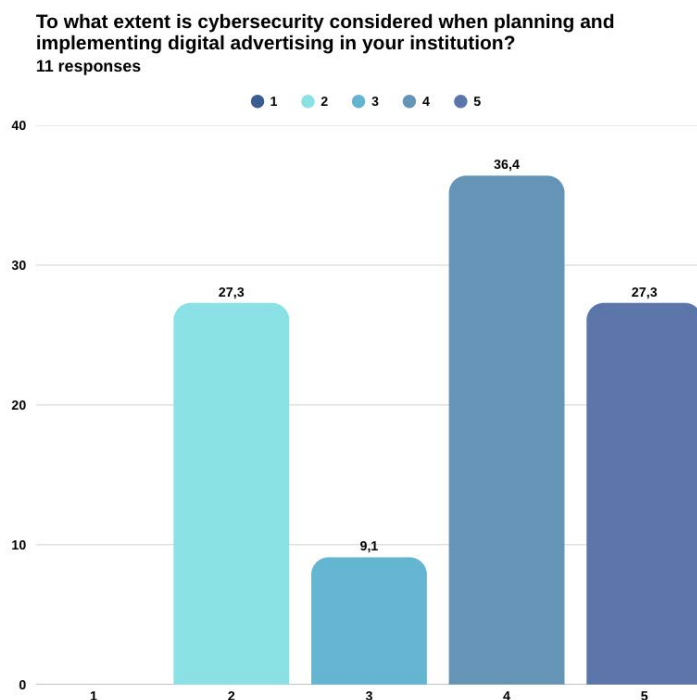
Do you perceive cybersecurity as a
barrier or a facilitator in digital
advertising?
11 responses



Source: Compiled by the author.

Chart 5 shows that respondents do not perceive cybersecurity as a limiting factor in digital advertising. A majority of respondents (72.7%) indicate that cybersecurity functions neither as a barrier nor as a facilitator. In contrast, 27.3% of respondents perceived cybersecurity as a facilitating factor, while none identified it as a barrier.

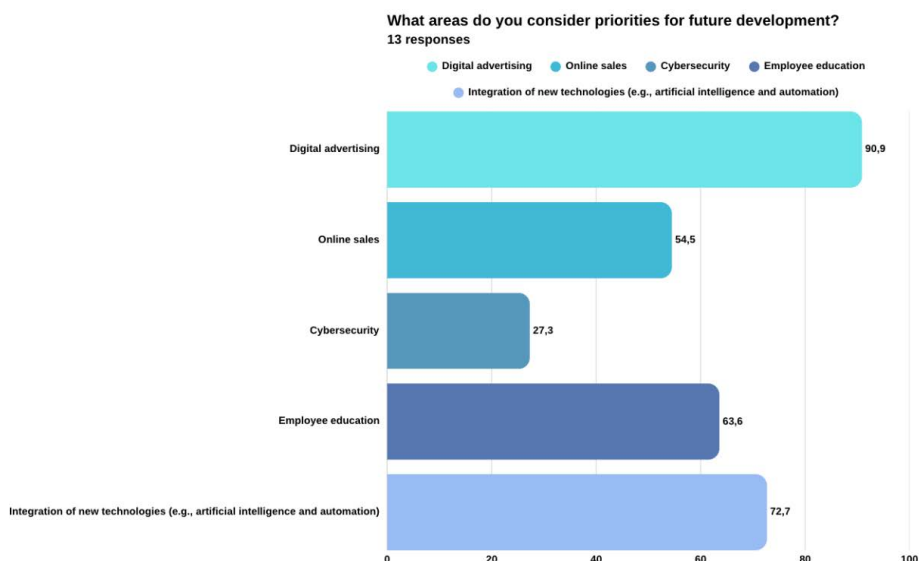
Chart 6: Level of cybersecurity involvement in the planning and implementation of digital advertising



Source: Compiled by the author.

Chart 6 shows that cybersecurity is mostly considered when planning and implementing digital advertising. The highest score of 4 was chosen by the majority of respondents (36.4%), while equal shares (27.3%) were recorded for the highest scores of 5 and 2. Score 3 was chosen by only 9.1% of respondents, while score 1 was not recorded. The above distribution indicates that cybersecurity plays a relevant role in digital advertising in most institutions, but differences in the level of integration are still visible.

Chart 7: Perception of priority areas for the future development of the institution



Source: Compiled by the author.

Respondents identify key priorities for future development in areas related to strengthening digital market presence. 90.9% of respondents singled out digital advertising, which indicates a high level of perceived strategic importance for the further development of institutions. New technologies such as artificial intelligence and automation (72.7%) and employee education (63.6%) are also considered extremely important areas. Online sales were identified as a priority in 54.5% of responses, which confirms their relevance in the context of the digitalisation of services. In contrast, cybersecurity was singled out in a smaller share, only 27.3%, which indicates that it is more often perceived as an integral part of the broader digital infrastructure.

The responses to the open-ended question: *“What do you consider to be the main challenges in integrating digital marketing and cybersecurity in the spa business?”* indicate several fundamental groups of challenges in integrating digital marketing and cybersecurity in the spa business. The most prominent theme relates to the protection of personal and particularly sensitive health data, which respondents recognise as a central issue when using digital marketing tools, online booking systems, and digital communication channels. This is directly linked to the need for compliance with the GDPR⁶⁴ (General Data Protection Regulation) and the secure

⁶⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

integration of various digital systems. The second group of challenges relates to organisational factors and human resources. Several responses emphasise the need for continuous employee education, the development of a security culture, and a clear definition of what to do in the event of a cyberattack. Therefore, it can be said that respondents do not view cybersecurity solely as a technical issue but as an area that depends on employees' competencies and the institution's organisational readiness. The third challenge relates to financial factors. Respondents state that the costs of implementing security systems are high. This indicates that the financial aspect represents an obstacle for those institutions with limited resources. In conclusion, the main challenges of integrating digital marketing and cybersecurity come down to three interrelated areas: data protection, employee education and the development of a security culture, and the financial challenge of implementing security systems in the institution.

5.3. Research Limitations and Recommendations for Future Research

The conducted research has several methodological limitations that need to be taken into account when interpreting the results. One of the key limitations of this research relates to the sample size, which includes a total of 13 respondents from health spas in Croatia and Slovenia, which limits the possibility of generalising the obtained results to the entire health tourism sector. This is partly due to the fact that the research is focused on a specific and relatively narrow population of experts employed in health spas, especially those who perform management, marketing, and related tasks, who are generally less available to participate in survey research. An additional limitation concerns potential response bias, as the research relies on respondents' statements about the practices and procedures within their institutions. Therefore, some responses may be shaped by subjective perception or by their level of information. The limitation of the research also stems from the research instrument itself. The questionnaire was developed specifically for this research and is not based on standardised multi-item measurement scales. This further indicates that the research is exploratory.

An additional limitation also applies to the comparative part of the paper, since two examples of health spas were selected for analysis, Terme Tuhelj (Croatia) and Terme Olimia (Slovenia). Therefore, the results of the comparative analysis should be interpreted as an insight into the selected cases, and not as a representative comparison of the Croatian and Slovenian health tourism sectors. The observed

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

similarities and differences relate exclusively to the analyzed institutions and can serve as a starting point for future research on a wider sample of institutions.

Accordingly, this research can therefore be considered preliminary and represents the basis for future research on a larger and more methodologically robust sample. Also, future research should include conducting in-depth interviews with management, marketing, or IT experts within the institutions, in order to gain a deeper insight into the organisational, financial, and regulatory challenges of integrating digital marketing and cybersecurity in health tourism.

Despite the aforementioned limitations, the results obtained provide valuable insight into the practice of digital marketing and cybersecurity in health spas and contribute to a better understanding of the researched issues.

6. CONCLUSION

The development of health tourism is increasingly linked to digital transformation processes, with digital marketing and cybersecurity forming two interconnected components of the modern spa business. Digital marketing plays an important role in visibility, communication, and market positioning, while cybersecurity represents a necessary framework for data protection, regulatory compliance, and maintaining user trust.

The results of the research, based on a small convenience sample, indicate that the health spas in Croatia and Slovenia recognise the importance of digital marketing and, at the same time, appreciate the need for secure management of digital processes. The findings suggest that digital channels are widely used for promotional and communication purposes, especially through official websites, social networks, and digital advertising. At the same time, the results indicate that the integration of digital marketing and cybersecurity in practice remains uneven, particularly in employee education, the implementation of security procedures, and investments in appropriate digital infrastructure. A comparative analysis of Terme Tuhelj and Terme Olimia showed certain similarities in the development of functional digital presence, but also differences in the intensity of content publishing, the dynamics of paid advertising, and the scope of multilingual adaptation. However, the aforementioned differences should be interpreted solely in the context of the analysed cases, and not as representative indicators of general differences between the Croatian and Slovenian health tourism sectors.

Given the limitations of the research, the non-representative sample, and the exploratory nature of the empirical part, the findings cannot be generalised to the entire health and wellness tourism sector. Therefore, they should be viewed as a

preliminary insight into the selected practices and perceptions of the respondents and as a starting point for further research. Future research should include a larger, more representative sample of institutions, the use of standardised measurement instruments, and more advanced statistical methods to enable a deeper analysis of the relationship among digital marketing, cybersecurity, and the competitiveness of health and wellness tourism institutions. Despite its limitations, the research points to the importance of an integrated approach in which digital communication, protection of sensitive data, employee education, and security procedures are integral to the responsible and sustainable digital business of health spas.

REFERENCES

BOOKS AND ARTICLES

1. Alarfaj, K. A.; Rahman, M. H., *The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix*, Applied Sciences, Vol. 14, No. 13, 2024, pp. 1-14
2. Bavrka, T.; Bošnjak, D., *Uloga digitalnog marketinga u promociji zdravstvenih usluga*, SKEI – Međunarodni interdisciplinarni časopis / International Interdisciplinary Journal, Vol. 5, No. 1, 2024, pp. 101–111
3. Belani, H. et al., *SWOT analiza informacijske i kibernetičke sigurnosti u zdravstvenim ustanovama Hrvatske*, Bilten Hrvatskog društva za medicinsku informatiku, Vol. 28, No. 1, 2022, pp. 1-13
4. Biloš, A.; Turkalj, D.; Kelić, I., *Micro-moments of user experience: An approach to understanding online user intentions and behavior*, CroDiM: International Journal of Marketing Science, Vol. 1, No. 1, 2018, pp. 57-67
5. Daries, N.; Cristobal-Fransi, E.; Ferrer-Rosell, B., *Implementation of website marketing strategies in sport tourism: analysis of the online presence and e-commerce of golf courses*, Journal of Theoretical and Applied Electronic Commerce Research, Vol. 16, No. 3, 2021, pp. 542–561
6. Elrod, J. K.; Fortenberry, J. L. Jr., *Advertising in Health and Medicine: Using Mass Media to Communicate with Patients*, BMC Health Services Research, Vol. 20, 2020, article no. 818, pp. 1-8
7. Florido-Benitez, L., *The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review*, Discover Computing, Vol. 28, No. 1, 2025, pp. 1-20
8. Fujs, D.; Bernik, I., *Analyzing cybersecurity of the European Union: Challenges and Opportunities for Public Administration*, Elektrotehniški vestnik, Vol. 91, No. 1–2, 2024, pp. 8-20
9. Geić, S., *Menadžment selektivnih oblika turizma*, Sveučilišni studijski centar za stručne studije u Splitu, Split, 2011
10. John, S.; Larke, R.; Kilgour, M., *Applications of social media for medical tourism marketing: an empirical analysis*, Anatolia, Vol. 29, No. 4, 2018, pp. 553–565
11. Kaur, K.; Kumar, P., *Social Media: A Blessing or a Curse? Voice of Owners in the Beauty and Wellness Industry*, The TQM Journal, Vol. 34, No. 5, 2022, pp. 1039–1056
12. Marine-Roig, E. et al., *Measuring gastronomic image online*, International Journal of Environmental Research and Public Health, Vol. 16, No. 23, 2019

13. Ravlić, S.; Unukić, I., *Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: Institucionalne i geopolitičke perspektive*, Festung: časopis za interdisciplinarna istraživanja u poslovanju, No. 2, 2025, pp. 143-149
14. Saeed, S. et al., *Digital Transformation and Cybersecurity Challenges for Business Resilience: Issues and Recommendations*, Sensors, Vol. 23, No. 15, article no. 6666, 2023, pp. 1-20
15. Saputra, A., *The Importance of Digital Marketing Integration in Strategic Management Planning*, Action Research Literate, Vol. 8, No. 5, 2024
16. Smith, M.; Wallace, M., *An Analysis of Key Issues in Spa Management: Viewpoints from International Industry Professionals*, International Journal of Spa and Wellness, Vol. 2, No. 3, 2019, pp. 119-134
17. Svete, U., *Cybersecurity between technological determinism, political governance and national security challenges*, Journal of Comparative Politics, Vol. 2, No. 2, 2025, pp. 107-125
18. Šolić, K.; Velki, T.; Matijašić Bodalec, D.; Fosić, I., *Comparative Study on Online Security Awareness and Behavior Among Healthcare Professionals in Croatia*, 2024 47th MIPRO ICT and Electronics Convention, IEEE, 2024, pp. 1803-1807, [<https://ieeexplore.ieee.org/abstract/document/10569325>], Accessed 11 March 2026

EU LAW

1. Council Recommendation (EU) 2025/C 3445 of 6 June 2025 on an EU blueprint for cyber crisis management, OJ C 2025/3445
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80
3. European action plan on the cybersecurity of hospitals and healthcare providers, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Directorate-General for Health and Food Safety, COM (2025) 10 final, Brussels, 15 January 2025
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 119/1
5. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L151/15
6. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) 2024 OJ L327/15
7. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 on measures to strengthen solidarity and capacities in the Union to detect, prepare

for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) [2025] OJ L38/1

NATIONAL REGULATION

1. Cybersecurity Strategy of the Republic of Slovenia (Strategija kibernetiske varnosti), Available at: [https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf], Accessed 11 March 2026
2. Decision on the adoption of the National Cybercrisis Management Program (Odluka o donošenju Nacionalnog programa upravljanja kibernetičkim krizama), Available at: [<https://ncsc.hr/hr/nacionalni-program-upravljanja-kibernetickim-krizama>], Accessed 11 March 2026
3. Information Security Act (Zakon o informacijski varnosti), Official Gazette of the Republic of Slovenia, No. 40/25
4. Cybersecurity Act (Zakon o kibernetičkoj sigurnosti), Official Gazette, No. 14/2024
5. National Cybersecurity Strategy (Nacionalna strategija kibernetičke sigurnosti), Official Gazette, No. 108/2015
6. Regulation on Cybersecurity (Uredba o kibernetičkoj sigurnosti), Official Gazette, No. 135/2024
7. Security and Intelligence System Act (Zakon o sigurno-obavještajnom sustavu) Official Gazette, No. 79/2006, 105/2006
8. Slovenian Tourism Strategy 2022–2028, May 2022, Available at: [<https://www.gov.si/assets/ministrstva/MGTS/Dokumenti/DTUR/Strategija-slovenskega-turizma-20222028-/SLOVENIAN-TOURISM-STRATEGY-2022-2028-v2.pdf>], Accessed 18 March 2026

WEB REFERENCES

1. All thermal spas and health resorts, Available at: [<https://slovenia-spa.si/all-thermal-spas-and-health-resorts-list>], Accessed 03 June 2026
2. Anson, A. et al., *Ransomware attacks on healthcare systems: Case studies and mitigation strategies*, 2023, Available at: [https://www.researchgate.net/publication/376514138_Ransomware_Attacks_on_Healthcare_Systems_Case_Studies_and_Mitigation_Strategies], Accessed 11 March 2026
3. Digital future for Europe, European Council, Available at: [<https://www.consilium.europa.eu/hr/policies/digital-transition/>], Accessed 04 March 2026
4. ENISA document with recommendations for cyber hygiene in health sector, Available at: [<https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber%20Hygiene%20in%20the%20Health%20Sector.pdf>], Accessed 04 March 2026
5. Information about the cyber attack on KBC Zagreb, Available at: [<https://www.dnevno.hr/vijesti/soa-se-oglasila-o-kibernetickom-napadu-na-kbc-zagreb-istice-mo-i-jos-jednu-vaznu-stvar-2466699/>], Accessed 17 February 2026
6. Lider, Europe searching for digital freedom, Available at:

- [<https://lidermedia.hr/zeleno-i-digitalno/digitalna-sloboda-europa-trazi-izlaz-iz-zamke-tehnoloskih-divova/>], Accessed 04 March 2026
7. Odebade, A. T.; Benkhelifa, E., *A comparative study of national cyber security strategies of ten nations*. 2023, [<https://doi.org/10.48550/arXiv.2303.13938>], Accessed 12 March 2026
 8. Official website of the National Centre for Cybersecurity about SK@ut system, Available at: [<https://ncsc.hr/hr/skaut>], Accessed 04 March 2026
 9. Information about the cyber attack on Slovenian pharmacies, Available at. [<https://net.hr/danas/svijet/hakeri-napali-slovenske-ljekarne-pao-centralni-informaticki-sustav-pacijenti-otezano-do-lijekova-a8c672a6-b9f2-11ec-a54f-0242ac130011?amp=1>], Accessed 11 March 2026
 10. Information about the cyber attack on Synnovis, Available at: [<https://www.england.nhs.uk/synnovis-cyber-incident/>], Accessed 11 March 2026
 11. Katalog projekata zdravstvenog turizma Ministarstva zdravstva Republike Hrvatske, Uprave za zdravstvenu zaštitu, Available at: [https://zdravlje.gov.hr/UserDocsImages/2025_Objave/Katalog%20projekata%20zdravstvenog%20turizma%202024..pdf], Accessed 03 June 2026
 12. Smith, M.; Puczkó, L.; Michalkó, G.; Kiss, K.; Sziva, I., *Balkan Wellbeing and Health tourism study*, 2016, Available at: [[BalkanWellbeingFINALREPORT.pdf](#)], Accessed 19 March 2026
 13. Telišman-Košuta, N.; Marušić, Z., *Percepcija Hrvatske kao destinacije zdravstvenog turizma na tržištu posrednika – kvalitativno istraživanje, Konačni izvještaj*, 2018, Available at: [https://www.htz.hr/sites/default/files/2019-07/Zdravstveni%20turizam_Percepcija%20Hrvatske_Konacni%20izvjestaj_23042018_FIN.pdf], Accessed 19 March 2026
 14. The Hipaa journal, Patient Death Linked to Ransomware Attack on Pathology Services Provider, Available at: [<https://www.hipaajournal.com/patient-death-linked-to-ransomware-attack/>], Accessed 04 March 2026