LegalTech Insurance[1]

Kamil Szpyt

„With great power there must also come great responsibility"
– Stan Lee[2]

1. Introduction

It is undoubtedly rare to begin considerations in the field of legal sciences with a quotation derived from the world of pop culture. At the same time, this maxim, although somewhat pompous, perfectly complements the thesis underlying this study. Moreover, since almost all of the articles contained in the present paper deal with issues that would have been considered pure science fiction only ten or twenty years ago, a slight reference to the realm of fantasy seems very appropriate here.

Coming of the crux of the matter: an analysis of press releases, popular science texts and even the majority of contemporary scientific publications may sometimes lead to the conclusion that LegalTech is an ointment without even one fly. It is almost always presented in glowing terms, with a long list of benefits that it brings not only to representatives of the legal sector, but also to all entities forced, to a greater or lesser extent, to seek assistance of lawyers[3]. Thanks to Legal Tech, the work of attorneys, notaries, legal department employees, etc. will ultimately become easier, faster, more efficient, and what is more, its quality will significantly increase.

The chances for the above vision to come true are undoubtedly high. However, one can get the impression that its proponents often completely ignore or disregard all (often serious) risks related to the introduction

1 The reasearch was financed from the funds earmarked for Statutory Activities of the Faculty WPAiSM/PRAWO/SUB/10/2020.

2 <https://archive.org/details/Amazing_Fantasy_vol1_15_201607/page/n13/mode/2up> accessed 25 April 2021.

3 See Jolanto Ojczyk, 'LegalTech to nieunikniona przyszłość prawników' <www.prawo.pl/prawnicy-sady/legaltech-day-podsumowanie,503668.html> accessed 25 April 2021.

of new IT solutions, such as increased risk of data being stolen by hackers from a poorly secured cloud or data loss due to failure of outdated software. There is never a hundred percent certainty that even the best solutions will not fail and the strongest security measures will not be broken. All the more so that LegalTech includes not only products of leading IT companies that meet demanding standards, but also - very often - debuting or even experimental software created by small start-ups or cheaper and more modest substitutes for computer programs offered by larger providers. We should not forget about the weakest link - people. Often untrained, tired and susceptible to manipulation[4].

According to the research conducted by BlueVoyant, in 2020 there was a surge in hacking attacks on law firms[5] and it seems that in 2021 this trend will not slow down at all[6]. This should come as no surprise, by the way - the legal sector has been among the top five sectors most attacked by cybercriminals for several years[7].

And here the question arises: are lawyers prepared for the worst possible scenario? That is, a situation in which, due to a lack of due diligence or as a result of sheer bad luck , confidential data of clients, contractors or the attacked party itself is lost/modified/disclosed, or the entire IT infrastructure of a law firm becomes blocked/destroyed? Undoubtedly, the consequences of such an incident can be truly dramatic: long-term paralysis of the law firm's operations, tarnished reputation that has been built up over the years, as well as enormous financial losses, including the costs of damages and administrative penalties.

4 Mitnick Security, 'The weakest link in safety is still man. Kevin Mitnick showed us how to outsmart us' <www.mitnicksecurity.com/in-the-news/the-weakest-link-in-safety-is-still-man.-kevin-mitnick-showed-us-how-to-outsmart-us> accessed 25 April 2021.

5 Krzysztof Sobczak, 'Coraz więcej cyberataków na firmy prawnicze' <https://www.prawo.pl/prawnicy-sady/cyberbezpieczenstwo-coraz-wiecej-atakow-na-firmy-prawnicze,505642.html> accessed 25 April 2021.

6 See Anita Błaszczak, 'Cyberprzestępczość: 2021 będzie rokiem wymuszeń w Internecie' <www.rp.pl/Biznes/201209783-Cyberprzestepczosc-2021-bedzie-rokiem-wymuszen-w-Internecie.html> accessed 25 April 2021.

7 Others are: medical industry, financial services, manufacturing and production, and government institutions; see: Dariusz Włodarczyk, 'Bezpieczny przedsiębiorca' (2018) 6 Miesięcznik Ubezpieczeniowy 87.

One of the basic preventive measures in this situation is taking out an appropriate insurance[8]. Its aim is to transfer the risk of negative financial consequences of the above-mentioned event to a third party, dealing professionally with such risk. The question is, whether the solutions used in this area for years are equally valid in today's reality - in the era of widespread use of new technologies in the legal sector? The present study aims to find an answer to this question

2. *Insurance in the Legal Sector - Past, Present and Future*

2.1. *The Past - Professional Liability Insurance*

Starting the consideration on insurance in law firms, it should be noted that it has become somewhat of a standard over the years that the lawyers running their own law firms have limited themselves to purchase only professional liability insurance. This type of insurance is intended for people who perform professions requiring high degree of specialization and carrying a risk of significant damage as a result of performing professional activities (both acts and omissions). This group, of course, includes virtually all legal professions whose representatives associate in self-governing bodies and operate in the free market, such as: attorneys, legal advisors, tax advisors, bailiffs[9], notaries and patent attorneys. Significantly, in many EU countries there is now an obligation for all or selected members of the a/m professions to take out compulsory professional indemnity insurance as a condition of lawful provision of services[10]. This is the case, for example, in

8 See more on the protective function of insurance: Malwina Lemkowska, 'Funkcje ubezpieczeń gospodarczych a zrównoważony rozwój' (2020) 2 Wiadomości Ubezpieczeniowe 50.

9 It seems that in the opinion of some people, the inclusion of the bailiff, who is - de facto - a public official, in the group of legal professions whose representatives operate in the free market, may arouse some controversy. However, looking at the issue from the practical, rather than merely doctrinal, perspective, such classification is - in principle - fully justified (at least in some EU countries, e.g. Poland).

10 Compulsory insurance is required for attorneys practicing in countries such as Italy, Spain, Germany, England, and Wales, among others; see Xymena Dyduch, *Zawód adwokata (abogado) w Hiszpanii*, in Michał Masior (ed), *Analiza prawno-porównawcza ustroju korporacyjnego wolnych zawodów prawniczych oraz rynku usług prawniczych w wybranych państwach, w kontekście regulacji i rynku w Polsce z uwzględnieniem dostępności obywateli do tych usług* (Instytut Wymiaru Sprawi-

Poland, Spain, Germany and Italy. It should also be noted that the Polish legal system does not provide for such an obligation for law graduates who do not belong to any of the above mentioned professional self-governments[11].

In practice, the aforementioned insurance serves to protect lawyers from the negative financial consequences of mistakes made at the stage of conducting court cases (e.g. failure to meet the deadline for lodging an appeal) or providing legal advice (e.g. indicating a solution based on outdated legal status)[12] and related to potential liability for damages. Over the years, this model of insurance has worked well, providing both lawyers and their clients with a relative sense of security.

However, with the increasing use of new technologies in the legal sector, especially LegalTech solutions, this situation has begun to change. To indicate its background, it is first necessary to clarify that in the activity of a law firm one can distinguish, so to speak, two areas within which an incident causing damage to a third party may occur:

---

edliwości 2018) 91 < https://iws.gov.pl/wp-content/uploads/2018/08/IWS-Masior-M.-i-inni-Wolne-zawody-prawnicze.pdf> accessed 25 April 2021; Michał Masior, *Wolne zawody prawnicze w Anglii i Walii oraz reforma ich regulacji*, 1. w Michał. Masior (ed) Analiza prawno-porównawcza ustroju korporacyjnego wolnych zawodów prawniczych oraz rynku usług prawniczych w wybranych państwach, w kontekście regulacji i rynku w Polsce z uwzględnieniem dostępności obywateli do tych usług, (Instytut Wymiaru Sprawiedliwości 2018) <https://iws.gov.pl/wp-content/uploads/2018/08/IWS-Masior-M.-i-inni-Wolne-zawody-prawnicze.pdf> accessed 25 April 2021 138.

11 Therefore, for the sake of clarity, in the following part of the article, when reference is made to law firms, it will only refer to firms run by representatives of one of the indicated professions (attorneys, bailiffs, notaries, etc.), whereas when reference is made to lawyers, it will refer to lawyers associated in one of the indicated professional self-governments, and not to graduates of law schools without professional qualifications. It should also be noted that, in the case of patent attorneys, referring to all members of the profession as lawyers may raise some doubts, since the law allows to practice this profession also persons with other, yet useful, education (economists, administrators, chemists, etc.). Nevertheless, taking into account that these persons are entitled to represent clients both in court proceedings and in administrative proceedings before appropriate state or EU bodies dealing with IP issues, a similar abbreviation seems acceptable.

12 For more on the civil liability of professional attorneys see Andrzej Rościszewski, Odpowiedzialność cywilna adwokatów (2014) 10 Palestra 7; Magdalena Bieluk, *Cywilnoprawna odpowiedzialność profesjonalnego pełnomocnika za błąd* (Uniwersytet w Białymstoku 2019) passim, <https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/8734/1/M_Bieluk_Cywilnoprawna_odpowiedzialnosc_profesjonalnego_pelnomocnika_za_blad.pdf> accessed 25 April 2021.

1) substantive - related to irregularities, already mentioned above, and resulting from the lawyers' negligence or lack of necessary competence in the scope of their legal practice;
2) technical[13] - concerning all kinds of failures in the duty to ensure security of the processed data, including document storage - disclosure of confidential information to an unauthorized third party (e.g. as a result of sending an unencrypted e-mail to the wrong addressee) can be indicated here as an example[14].

As recently as a few or a dozen or so years ago, the predominant risk was that errors would occur in the substantive area. Technical incidents were relatively rare and were usually related to the carelessness of lawyers or their employees, which manifested itself, for example, in losing case files during their relocation. The introduction of new technologies, especially LegalTech solutions, into everyday work in law firms seems to reverse these proportions. On the one hand, lawyers gain new tools to support their competencies and improve the quality of their services: legal information systems equipped with letter templates and case law compasses, computer programs that check the content of a contract, or even systems based on artificial intelligence that can predict the outcome of a future lawsuit. As a result, the number of substantive mistakes will undoubtedly decrease over time. On the other hand, lawyers often lack elementary knowledge of cybersecurity and make cardinal mistakes in this area, e.g., using computers with outdated operating systems, unprotected with antivirus software, or using commercial email providers' services that are not adapted to the requirements of the legal industry[15]. And we are discussing only some basic IT tools. If we couple this with the constant improvement of methods used by hackers to break through security measures, it turns out that in the coming years, the probability of stealing poorly protected client data will be several (dozen / several dozen?) times greater than the

13 See Christian Zimmermann, 'Legal Tech – Vielfalt der Anwendungen und richtige Haftungsvorsorge', 815 <https://anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/anwaltsblatt-online/2019-815.pdf> accessed 25 April 2021.

14 Of course, such an outlined division can hardly be considered rigid. In some cases, such as those involving the disclosure of professional secrets, it seems that similar incidents can be classified as both substantive and technical, or their nature changes over time and shifts from one to the other.

15 On the practical aspects of securing data in a law firm see Dariusz Szostek (ed), *Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/adwokackiej/notarialnej/komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej* (Wydawnictwo C.H.Beck 2018).

risk of an attorney at law bringing an action based on a legal basis that is no longer valid. We should also add the risk of a long-term downtime in the law firm's operations due to IT system interference, or even the need to recreate the collected data in case of encryption thereof[16].

In the light of the foregoing, the question arises whether traditional professional liability insurances are able to protect law firms from the negative consequences of such attacks. Some of them are, to a certain limited extent. For example, professional liability insurance offered by AXA Ubezpieczenia Towarzystwo Ubezpieczeń i Reasekuracji S.A. covers, among others, damage caused by improper edition of documents, as well as loss, distortion, damage and improper transmission of information (including by electronic means), as well as damage resulting from hacking into the insured entity's computer system by a third party[17]. However, in general insurance terms and conditions of a similar product offered by Aviva Towarzystwo Ubezpieczeń Ogólnych S.A., there is an exclusion stating that the insurer is not liable for data loss[18]. In other words, protection against the aforementioned damages is by no means an obligatory element of such insurance and its provision will always depend on the content of a specific agreement as well as general insurance terms and conditions.

Incidentally, it is worth mentioning that the situation will be no better for any entities established by (and associating) lawyers who do not belong to any of the above-mentioned self-governments. Similar entities, most often functioning in the form of limited liability companies (e.g. insurance claim and debt collection law firms), in practice usually take out liability

16 Of course, it is important to mention that not all incidents of a technical nature will be the responsibility of the law firm and its affiliated lawyers. One should not forget about mistakes made by IT entities providing services to the law firm, e.g. in the form of a cloud solution. In such a situation, they will be held liable, possibly - in their place - the insurer. It is worth mentioning that representatives of the aforementioned industry usually use IT liability insurance dedicated to them.

17 Paragraph 1 Section 3 'Warunki Ubezpieczenia. Ubezpieczenie odpowiedzialności cywilnej zawodowej' <www.uniqa.pl/fileadmin/produkty/centrum_klienta/dokumenty/540_WU.pdf> accessed 25 April 2021; currently AXA Ubezpieczenia Towarzystwo Ubezpieczeń i Reasekuracji S.A. merged with UNIQA Towarzystwo Ubezpieczeń S.A.

18 Pkt 10.5 'Ogólne Warunki Ubezpieczenia odpowiedzialności cywilnej z tytułu wykonywania zawodu' <https://www.aviva.pl/ubezpieczenia-dla-firm/ubezpieczenia-korporacyjne/ubezpieczenia-OC-zawodowe/ubezpieczenie-OC-zawodowe> accessed 25 April 2021.

insurance for the conducted business activity. As a rule, it does not provide for the possibility of covering the risk of data loss or hacking attack[19].

However, returning to the issue of professional liability insurance: in view of the findings to date, it is undoubtedly necessary to increase the awareness of lawyers, so that when taking out professional liability insurance, they would choose those policies which also cover the above-mentioned damages[20]. At the same time, it is difficult to hide the fact that even this solution will be insufficient. Civil liability insurance, by its nature, covers only damage suffered by third parties, not the entities insured themselves. Therefore it does not cover such negative consequences as the need for a law firm to restore lost data, secure the system or pay administrative fines. The costs of these activities may also exceed the law firm's financial capabilities. Thus, it can be assumed that, although professional liability insurance is an indispensable element of any lawyer's business, it should be complemented by insurance that provides protection also for the damages incurred by the law firm itself.

And here comes the key issue: what kind of insurance should it be? Even a cursory analysis of the market will show that there is no insurance dedicated to LegalTech solutions. At least - for the time being. It is another matter whether it is really needed when its role is played by so called cyber risk insurance. And it is cyber risk insurance that will be discussed in the next subchapter.

2.2. The Present - Cyber Risk Insurance

Cyber risk insurance is also often referred to as cyber insurance[21] or data insurance[22]. The latter term is inaccurate, as these insurance policies some-

19 'Cyber ubezpieczenia a inne polisy' <https://broker.andiw.pl/cyber-ubezpieczenie-broker-ubezpieczeniowy-ubezpieczenie-cybernetyczne/> accessed 25 April 2021.

20 This is assuming, of course, that they have a say in the matter. For it may be that in a particular state or law corporation, insurance for lawyers affiliated with the self-regulatory body is negotiated and purchased by its governing body.

21 See Christian Zimmermann (13) 816.

22 Sometimes they are even colloquially referred to as GDPR "insurance" or "GDPR risk insurance", which is supposed to refer to GDPR. This should not come as a surprise as the coming into force of the aforementioned legal act was undoubtedly a strong impulse for cyber risk insurance market development. Therefore, even in the offers of some insurers, one may come across "special treatment" of personal data issues. As an example, we can mention the "CYBER GUARD" insurance of Colonnade Insurance S.A. (admittedly described in the general conditions of in-

times cover incidents that have little to do with data breaches, such as the publication of material on a website infringing a third party's copyright[23].

Consideration on the subject of insurance should begin with an explanation of what this "cyber risk" really is. Contrary to appearances, it is not that simple. This is because at the current stage the term "cyber risk" has neither legal, nor a commonly accepted definition[24]. Among the many definitions present in the literature, the one proposed by The Geneva Association is worth mentioning, according to which the a/m term means any risk resulting from the use of information and communication technologies, which assumes confidentiality, availability and integrity of data or services[25].

The source of loss in the aforementioned insurances can be primarily:

1) an intentional external attack (e.g. hacking into an IT system by a hacker);
2) intentional internal attack (e.g. transfer of data by disloyal employee);
3) accidental losses (e.g. human error - mistaken deletion of data, loss or destruction of data carrier)[26].

---

surance as "liability insurance for incorrect handling of information", but actually being insurance against cyber risks). The product in question is available in two variants: a broader one (covering the full catalog of cyber risks) and a narrower one (covering only the issue of personal data law breach - "RODO GUARD"). This clearly proves that in the opinion of the insurance company the second issue may be much more important for the clients and therefore it is justified to purchase insurance variant limited only to it; see 'CYBER GUARD. Ogólne warunki ubezpieczenia odpowiedzialności za nieprawidłowe postępowanie z informacją' <https://colonnade.pl/files/file_items/Og%C3%B3lne%20warunki%20ubezpieczenia%20CYBER%20GUARD%2025.05.18_0.pdf> accessed 25 April 2021 and 'RODO GUARD. Ogólne warunki ubezpieczenia odpowiedzialności za dane osobowe' <https://colonnade.pl/files/file_items/Og%C3%B3lne%20warunki%20 ubezpieczenia%20RODO%20GUARD%2017.06.19.pdf> accessed 25 April 2021.

23 'Cyber ubezpieczenia a inne polisy' <https://broker.andiw.pl/cyber-ubezpieczenie-broker-ubezpieczeniowy-ubezpieczenie-cybernetyczne/> accessed 25 April 2021.

24 See Katarzyna Malinowska, 'Aspekty prawne ubezpieczenia cyber ryzyk' (2018) 2 Prawo Asekuracyjne 16.

25 The Geneva Association, 'Ten key questions on Cyber Risk and Cyber Risk Insurance', 12, <https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf> accessed 25 April 2021.

26 Simon Cooper, *Cyber Insurance*, w: Peter Rogan (ed.), *The Insurance and Reinsurance Law Review* (Law Business Research Ltd 2020), <https://thelawreviews.co.uk/title/the-insurance-and-reinsurance-law-review/editors-preface> accessed 25 April 2021; another common, dichotomous division is: by source (external

The literature indicates that for a long time the protection against cyber risks was partly provided by other types of insurance: property insurance[27], business interruption insurance[28], general liability insurance and professional liability insurance. However, as the aforementioned insurances were not constructed strictly in order to protect against the negative effects of cyber risk, despite some substantive compatibility, their scope was not adjusted to the specificity of the risk, which resulted in exclusion of the insurer's liability in case of the most critical episodes[29]. As a result, even now the scope of cyber risk insurance may overlap with other types of insurance, but it will concern only small parts[30].

Cyber risk insurance as a separate product in many countries (including Poland) is still developing and trying to gain more popularity. In other countries it has been appreciated and used more widely for years (e.g. USA)[31]. Cyber risk insurance should undoubtedly be classified as property insurance, however, it is not possible at the moment to point out one main model of its construction. Although some unification is taking place, it is still quite a diverse insurance of a complex nature. In more general terms it can be stated that the protection covers both civil liability as well as own costs incurred by the insured in connection with an incident. To be more specific, cyber risk insurance usually consists of several segments/sections, among which the following can be pointed out as the most important ones:

1) civil liability related to violation of the right to privacy and personal data - including, in particular, the costs of damages and compensation for the disclosure or loss of personal data, as well as other forms of violations of privacy[32]. In addition to this, the said section should also

---

and internal) and by cause (intentional attack and negligence of the insured/his employee).

27 On property insurance see Bartosz Kucharski, *Świadczenie ubezpieczyciela w umowie ubezpieczenia mienia* (Wolters Kluwer 2019).

28 On business interruption insurance see Jerzy Sawicki, 'Ubezpieczenie Business Interruption (BI) jako zabezpieczenie przyszłych dochodów przedsiębiorstwa' (2008) 7 Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania. 37–48; Agnieszka Szewczuk, 'Business interruption: ewolucja kompleksowego programu ubezpieczeniowego dla sektora małych i średnich przedsiębiorstw' (2010) 50 Ekonomiczne Problemy Usług 521–528.

29 Malinowska (n 24) 22.

30 Cyber ubezpieczenia a inne polisy' (n 23).

31 Michał Molęda, 'Cyber is the new black' (2018) 6 Miesięcznik Ubezpieczeniowy 80.

32 ibid 81.

include, among other things, the costs of notifying the affected persons of the incident, removing their data from the network and the costs of restoring the removed data[33];

2) administrative penalties - one of the most important and highest rated elements of this type of insurance. As you can easily guess, it will be applied mainly to administrative penalties imposed for violation of data protection regulations. Therefore, as it was already mentioned in the footnote, in practice the market offers products that are a "sliver" of the full cyber risk insurance and cover only the above mentioned area (e.g. "CYBER GUARD Colonnade Insurance S.A.");
3) the costs of IT incident handling activities - these costs usually refer to acting on three levels and providing assistance in three different areas: IT, legal and public relations. The insurance may either cover the costs of using specialist service in these areas chosen by the insured or provide assistance of entities cooperating with the insurer on a permanent basis[34]. This section is extremely important as it is often both very difficult and expensive for the insured to find similar ad hoc assistance. The IT team may be requested, for example, to analyze whether the encrypted data can be recovered, or whether it is "worth" recovering, or whether it would be cheaper to pay the ransom. When it comes to the legal team, the question may arise whether law firms will actually be interested in using "external" lawyers. After all, they should have their own employees with the necessary expertise in this area. That is, by all means, a major fallacy, which can be supported by three arguments. Namely: the support provided by such teams provides an appropriate distance to the conducted case (due to the fact that it does not concern the lawyers personally), specialist knowledge (since the attack could have taken place, for example, on a law firm specialized in tax or family law, whose representatives do not have the slightest knowledge of the potential legal consequences of cyberattacks), as well as own equipment, i.e. computers, legal programs, etc. (this is especially important when the attack took place on a law firm specialized in

33 ibid.

34 Of course, this is not a closed catalog. Some insurances (e.g. Cyber ERM 2 offered by Chubb Limited) provide, for example, the assistance of an investigator or a credit specialist (usually - for a specified period of time), who is to advise no longer the insured person himself, but individuals whose data has been disclosed as a result of a cyber-attack; see 3.17 Letter G Ogólne warunki ubezpieczenia <www.chubb.com/content/dam/chubb-sites/chubb-com/pl-pl/products/cyber/documents/pdf/owu-cyber.pdf> accessed 25 April 2021.

tax law). This is particularly important when a law firm's IT system has been hacked and locked/encrypted);

4) civil liability related to the operation of an IT system - theoretically, the scope of this segment coincides with that of section 1); in practice, however, it may concern damages reaching far beyond the sheer data leakage. As an example, a client's or contracting party's computer may be infected with incoming files, which may result in incurring costs of using an IT specialist (which will no longer be the law firm's self-inflicted damage, but third party's)[35];
5) multimedia liability - this segment deals with liability coverage for publications through electronic means (e.g., websites, social media or intranet)[36];
6) ransomware costs in case of cyber extortion - the insurer's ability to cover ransomware costs is usually subject to the insurer's prior approval. This is usually preceded by a process of analysis of a specific situation by the already mentioned IT team, which verifies whether in a given case an "honourable" hacker group is behind the attack (i.e. a group which, having received the demanded money, will provide a program to decode data) or not (i.e. a group which will not fulfill its part of the "agreement" and the money spent on the ransom will be wasted). Usually, the payment of the ransom is realized in one of the cryptocurrencies[37];
7) costs of data restoration and downtime costs - in this case we are no longer talking about the data of third parties (e.g. clients), but the data of the law firm itself. Moreover, the said section also covers downtime costs related to the fact that e.g. malware overloaded the servers[38].

Of course, this type of insurance does not cover all damages. As almost every type of insurance, it involves a number of exclusions. The most common exclusions are usually related to the negligence of the insured entity in applying appropriate information system protection rules (principles):

---

35 Michał Molęda (n 23) 82.
36 ibid.
37 More about the issue of cryptocurrencies and related legal issues see Paweł Opiłek, 'Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego' (2017) 6 Prokuratura i Prawo 36–59; Krzysztof Markowski, 'Kryptowaluty. *Powstanie-typologia-charakterystyka*' (2019) 3 Civitas et Lex 69–82
38 See the similar systematics proposed by Michał Molęda (Michał Molęda (n 31) 81).

1) failure to encrypt data that has been lost;
2) storing data on a device that was not equipped with appropriate security software (especially anti-virus software);
3) lack of care for infrastructure, i.e., use of outdated devices, improperly enabled/connected;
4) lack of software updates[39].

The exclusion most often will also cover data loss resulting from cyber-terrorist activities[40].

In the light of the above considerations, it should be said that the pandemic and the associated progressive digitization as well as transfer of activities to the network will undoubtedly increase the interest in cyber risk insurance in all industries. At the same time, it is the legal industry, so keen to move with the times and use LegalTech solutions in its business, that should be among the first to become interested in cyber risk insurance. This solution may bring numerous benefits. First and foremost, it allows for faster engagement of appropriate financial means and substantive support, which - perhaps - would not be immediately available to a particular law firm, and which will allow to minimize or completely eliminate the negative effects of a cyber incident[41]. Additionally, and also noteworthy, the insurance itself to some extent also increases the security of data in a law firm. In many cases, the policyholder will have to meet a number of strict conditions regarding, among others, data security, employee training, etc. in order to be able to enter into the agreement and - in the event of an incident - benefit from the insurance. This forces the policyholder to be extra diligent in this regard[42].

To sum up: it seems that cyber risk insurance should become an obligatory element of "equipment" for law firms that want to use LegalTech solutions in a really responsible and professional way.

---

39 See Paragraph 9 Section 7 'Ogólne Warunki Ubezpieczenia od Ryzyk Cybernetycznych' - insurance offered by Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A <http://cyberochrona.ergohestia.pl/wp-content/uploads/2015/10/OG%C3%93LNE-WARUNKI-UBEZPIECZENIA-OD-RYZYK-CYBERNETYCZNYCH2.pdf> accessed 25th April 2021.

40 See Jacek Zębala, 'Wybrane problemy ubezpieczeń cyber risk' (2018) 6 Monitor Ubezpieczeniowy 85.

41 *ibid.*

42 We are dealing with an analogous situation, e.g. in the case of car insurance, in which one of the conditions for the payment of compensation for a stolen vehicle may be the proof of parking the car in a guarded parking lot.

2.3. *The Future - Civil Liability Insurance of Artificial Intelligence System Operator*

A certain part of LegalTech solutions is based on - more or less - advanced artificial intelligence systems. Therefore, when writing about insurance in LegalTech, one cannot fail to mention the planned introduction of a new, mandatory civil liability insurance provided for artificial intelligence (AI) operators. The enactment of this type of insurance is stipulated by the draft regulation annexed to the Resolution of the European Parliament of 20.10.2020 with recommendations to the Commission on the system of civil liability for artificial intelligence [2020/2014(INL)][43]. This act, entitled Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems, would be intended to unify the rules of liability and insurance of AI within the EU. For the purposes of the a/m act, the European Parliament provided a new definition of an AI system, according to which it is a system that is based on software (possibly embedded in a device), that exhibits behavior simulating intelligence (i.a. by collecting and processing data, analyzing and drawing conclusions regarding the environment) and takes actions which are autonomous to a certain extent, aiming to achieve a specific goal.

The draft regulation distinguishes between two types of AI systems: high-risk and high-risk-free. "High risk" is understood as "a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected", whereby "the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used "[44].

According to the draft regulation, the operator of a high-risk AI system should be liable on a strict liability basis for any damage caused by a physical or virtual operation, a physical or virtual operation of a device, or a physical or virtual process using an artificial intelligence system, while an operator of an AI system that is not a high-risk system should be held liable on the basis of presumed guilt.

---

43 <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html> accessed 25 April 2021.

44 Article 3 Letter c draft Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems.

With the above in mind, there is a question of clarifying the term "operator". The draft regulation indicates that both frontend and backend operators will be considered operators. The former term refers to a natural or legal person who controls the risks associated with the operation of an artificial intelligence system to some extent and benefits therefrom, while the latter one should be understood as referring to "natural or legal person who, on a continuous basis, defines the features of the technology and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system"[45].

The EP believes that one of the conditions for AI to succeed in the future is to guarantee coverage for liabilities related to the damages and losses caused thereby. This guarantee can be achieved by introducing mandatory civil liability insurance for the operators of high-risk AI systems. In the case of a front-end operator, the liability insurance would cover the operation of the AI system, and in the case of a back-end operator, the insurance for the activity or product should cover services offered by that product[46].

Ultimately, all high-risk systems would be included in an exhaustive list in an appendix to the envisaged regulation. The list would be reviewed and modified every six months to respond as quickly as possible to the technological developments and the introduction of new products approved for the market. In order to provide the entrepreneurs and research organizations with a sense of certainty in planning and investment process, changes to the list of critical industries should only be made every twelve months.

The regulation also specifies the maximum amounts of compensation, which undoubtedly translated into the amount of cover in the insurance taken out. Namely, the operator of a high-risk artificial intelligence system is liable for the following damages:

1) up to a maximum amount of two million euros in the event of death, injury or mutilation of a person as a result of the operation of a high-risk artificial intelligence system;
2) up to a maximum amount of one million euros in the case of serious intangible damage resulting in verifiable economic loss or damage to property, including the destruction of several objects belonging to the

45 Article 3 Letter d-f draft Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems.

46 Article 4 Section 4 draft Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems.

> victim as a result of a single operation of a one high-risk artificial intelligence system; where under the contract the aggrieved party also has a right to claim against the operator, no compensation will be payable under the future regulation if the total value of the destroyed property or serious intangible damage does not exceed five hundred euros.

The above solution should undoubtedly be considered as raising a lot of doubts and creating significant complications for the insurance industry (related, among others, to risk estimation[47]). Detailed analysis of these complications goes beyond the framework of this research paper. The issue that should be noted, however, is the lack of exclusions for specific industries, including the legal sector. As a result, it should be recognized that the above regulations will also apply to LegalTech solutions whose operation is based on artificial intelligence. In some cases, this will necessitate the purchase of additional insurance.

It is also worth pointing out that the described situation may also result in lawyers attempting to attribute certain actions to themselves, even though these actions were carried out by artificial intelligence. For example, software used to estimate optimal compensation and punitive damages and to draft lawsuits in medical cases. Even if it was not considered a high-risk AI system, it would still give rise to liability on the basis of presumed guilt, that is, less favorably than in case of liability for the actions of a "real" lawyer (for in the latter case, the liability is established on the basis of guilt). Hence, the average lawyer would often prefer to point out that he himself is the author of the solutions in question, particularly if he had not previously taken out AI operator liability insurance (which is not supposed to be compulsory in the case of AI systems other than high-risk systems).

3. Summary

The main conclusions that can be derived from the above considerations are as follows: professional liability insurance for lawyers should not be

47 See Grzegorz Dybała and Kamil Szpyt, 'Odpowiedzialność odszkodowawcza za sztuczną inteligencję' (2021) 5 Gazeta Ubezpieczeniowa 19; Marcin Amrosz, 'Sztuczna inteligencja z obowiązkowym ubezpieczeniem OC?' (2021) 5 Miesięcznik Ubezpieczeniowy 52–53; more general comments about AI insurance see: Dariusz Smoloń, Oskar Sokoliński and Gustaw Szarek, 'Polisa od sztucznej inteligencji' (2018) 10 Miesięcznik Ubezpieczeniowy 34-36.

considered a sufficient solution for law firms wishing to use LegalTech solutions on a larger scale. The extent of damages that can be suffered by both the insured, as well as his clients and contractors, goes well beyond the scope of protection provided by this type of insurance. Searching for an answer to the question how to fill this gap, it should be stated that for the moment there is no insurance policy intended specifically for LegalTech solutions available on the market and, moreover, there is no need for it to be introduced. This role is being successfully performed by Cyber risk insurance and it seems reasonable to popularize and recommend its wider use. Ultimately, it could be a good supplement to the mandatory professional insurance taken out by attorneys, notaries, patent attorneys, bailiffs and tax advisers. On the other hand, the introduction of a new compulsory civil liability insurance for AI system operators is likely to cause a lot of confusion. The provisions presented in the draft raise considerable doubts, which will be increased by the risk of duplication of protection offered by these provisions with that guaranteed by professional liability insurance and cyber risk liability insurance.

To sum up the whole discussion so far, it is worth recalling once again the opening quotation of this research paper: "with great power there must also come great responsibility". In the context of the considerations presented so far, it may be understood both literally, as a warning against the risk of inflicting considerable damage to the client, which may then result in a law firm being sued, as well as metaphorically - as a reminder of the lawyers' responsibility for their clients who entrusted them with their secrets. In either case, however, it is hard to ignore the message of the aforementioned quotation.