

Edyta Tkaczyk*

Cyberspace and public access to the legislative process

Abstract

Public access to the legislative process is one of the principles governing Parliamentary law. This process primarily entails public debates, the public nature of motions and submissions, public voting, the public adoption of resolutions, and the public availability of documents constituting the basis for the work of the Sejm – the Lower House of Parliament. Thanks to modern means of communication and live broadcasts, the public has unrestricted access to Parliamentary debates and the legislative process. While searching for, or generating, information by automated means, recipients can follow the legislative process in the form of video broadcasts. Therefore, all types of Internet attack constitute a clear threat for the validity of the legislative process, and can lead to the disruption of information disclosure as part of the public debate.

Key words: legislative process, public-access principle, Parliamentary law, cyberspace, legislative information

* Edyta Tkaczyk Ph.D., The Institute of Law, Administration, and Security, Warsaw Management University, e-mail: edytatkaczyk13@wp.pl, ORCID: 0000-0001-9831-6430.

One of the most significant consequences of the emergence and rapid development of the information society is the extension of the material scope of State security by the principle of public access to the legislative process. Access to information, and the capacity for processing, securing, transmitting, and storing such information, is becoming central to State security in the Internet space¹. Information has become a strategic resource in cyberspace, and its significance has increased considerably, notwithstanding its presentation and storage forms². Public access to the legislative process is one of the principles governing Parliamentary law. It can be currently treated as a characteristic of the institution of Parliament itself, as a kind of a Parliamentary law standard. It constitutes one of the elements in the representative character of Parliament, allowing the public to observe the operating methods accompanying the procedures³.

The principle of public access to the legislative process was laid down in the Constitution, which makes it a well-established rule.

Under the applicable Constitutional law, public access to the legislative process should be discussed against a backdrop of the characteristics of the legislative process itself. First, the principle of public access to the legislative process is expressed in the provisions under which Poland is a democratic State based on the rule of law, and in the representative function of the Sejm and the Senate⁴. Second, the legislative process is not kept secret from the public. The public-access principle can also be inferred from the provisions of Article 61 of the Constitution, under which Polish citizens have the right to obtain information on the activities of public authorities.

The public-access principle relates to both the Sejm and the Senate.

It covers the sessions of the Sejm. This means that, most of all, it can be applied to all Parliamentary procedures in the field of legislation, i.e. to the Praesidium of the Sejm, the Council of Elders, and the Sejm Committees. Under

1 See Directive (EU) 2016/1148 of the European Parliament, and of the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (OJ EU L 194 of 19 July 2016, p. 1).

2 A. Letkiewicz, *Istota współczesnego zarządzania jako element bezpieczeństwa*, [in:] *W kręgu nauki o bezpieczeństwie*, red. M. Jurgilewicz, S. Sulowski, Warszawa 2018, p. 198 et seq.

3 M. Stębel, *Rola polskiego parlamentu po transformacji ustrojowej*, [in:] *XV lat obowiązywania Konstytucji z 1997 r. Księga jubileuszowa dedykowana Zdzisławowi Jaroszowi*, red. M. Zubik, Warszawa 2012, p. 159.

4 M. Leszczyński, *Spółeczeństwo „zatomizowane” jako skutek rozpadu tradycyjnych wspólnot. Implikacje dla współczesnego bezpieczeństwa*, [in:] *Prawne, instytucjonalne i społeczne uwarunkowania bezpieczeństwa*, red. S. Bębas, A. Gołębiowski, Radom 2014, p. 26.

Article 110 (1) of the Constitution, the Sejm and the Senate hold debates in sessions. It should be understood as everything which happens in the meeting room from the time the Marshal of the Sejm opens a session to the time the session is closed.

Public access to the legislative process primarily entails public debates, the public nature of motions and submissions, public voting, the public adoption of resolutions, and the public availability of documents constituting the basis for the work of the Sejm. All this is published and uploaded onto the Parliament website, www.sejm.gov.pl.

The manifestation of the principle is public access to Bills, Statements of Reasons, reports on the sessions of the Sejm and Committees, and video recordings.

Against a backdrop of Polish Parliamentary traditions, it should be assumed that public voting provides the people with an opportunity not only to track the course of such procedures, but also to learn how the deputies vote.

Voting on Bills is the most important part of sessions, and the electorate cannot be denied information on the choices their representatives make.

Public access to the legislative process includes, first and foremost, the principle of public access to debates, which involves the citizens' observing the work of Parliament live, and obtaining relevant information via other mass media. First, it is related to the broadly understood freedom-of-the-press principle (Article 14) and access to information (Articles 61 and 214). Second, it includes access to documents and materials which are part of the legislative process. Third, it means access to materials and documents with records of the on specific Bills, in particular stenographic records and the printed materials issued by the Parliament.

The principle of public access to the legislative process creates specific rights on the part of citizens, and on the part of mass-media representatives. Such types of activity pursued by public television and radio broadcasters can be regulated by way of an ordinary Act, as there are no explicit constitutional provisions which would state otherwise.

The fact that the authority to enact laws was given to the Sejm (Articles 118 (3), 120 (1) and 121 (1) of the Constitution) should be understood as the obligation to initiate the legislative procedure by putting forward a Bill in the Sejm, followed by the motion for a given Act solely by the Sejm during a plenary session, and not by any of its internal bodies.

Public access to work on Bills is referred to in Article 113 of the Constitution, and it would seem that there is no explicit provision which would extend the application of this principle to the work of committees.

The principle of public access to three readings is the outcome of the legislative-procedure model in place in the Republic of Poland, consisting of multiple debates on Bills held by a House of Parliament before a given Act is passed in its final form, as laid down in Article 119 (1) of the Constitution, and defines the internal legislative-procedure model in place at the Sejm⁵.

The principle of public access to three readings is referred to in the Constitution only with regard to Parliamentary procedures. This process includes an obligation to follow the procedure in such a way that it is based on readings. Moreover, the question might be posed whether the interpretation of the term “reading” also refers to the extension of the public-access principle to the work of committees⁶.

Thanks to modern means of communication, and live broadcasts of Parliamentary debates and the legislative process, the public is given information not only about the work of Parliament, but also about the views expressed by its elected representatives, and about their engagement in addressing specific social issues. It creates extraordinary feedback, and allows the dissemination of socially acceptable views expressed by Members of Parliament about legislative initiatives⁷. All this results in the fact that Parliament, as a legislative body, is expected to provide maximum public access, whereas confidentiality can be associated with the operations of other State authorities, in particular the executive branch⁸.

At present the public-access principle includes not only the access by visitors to the audience gallery, but also live broadcasts from the sessions, and reports on the progress on the work on a given Bill. Given such understanding of public access to the legislative process, it can be stated that this principle is significant, not only for informing the public directly about Parliamentary business, but also for reaching specific political goals and the goals of individual MPs, or the parties they represent.

5 L. Garlicki, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, vol. 2, Warszawa 2001, p. 2.

6 J. Jaskiernia, *Zasady demokratycznego państwa prawnego w sejmowym postępowaniu ustawodawczym*, Warszawa 1999, p. 180 et seq.

7 B. Szepietowska, *Proces ustawodawczy*, [in:] *Parlament model konstytucyjny a praktyka ustrojowa*, red. Z. Jarosz, Warszawa 2006, p. 100 et seq.

8 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, p. 570.

Most Parliaments allow the presence of radio and television representatives during sessions, including plenary sessions and the meetings of some Parliamentary bodies, in particular investigative committees and standing committees with investigative powers.

It should be stressed that Sejm sessions are open to the public, but the deputies may decide to hold in-camera sessions if the good of the State requires such a procedure. The pace of a given legislative procedure cannot in itself constitute grounds for rendering it unconstitutional. First of all, constitutionality can be assessed in terms of the influence the procedure exerts on the pluralist nature of Parliament, i.e. by reviewing whether the course of Parliamentary business has not denied the public their right to follow legislative proceedings⁹. Second, it can be evaluated from the perspective of the correlation between the fast pace of legislative work and the quality of laws. However, the latter aspect is reviewed, in the course of proceedings, by assessing the substantive value of legal provisions as part of the conducted legislative process. There is a possibility that an Act which was debated and adopted hastily can contain errors, but these should not be decisive factors when evaluating the compliance of the Act with the Constitution.

The provisions of the Constitution do not regulate legislative procedures in full, including their online presentation¹⁰. In line with the Principle of Sejm autonomy, such issues should be governed by Rules & Regulations, whereas the Constitution only formulates certain general principles, and governs issues of material importance. The principle of public access to the legislative process should be classified as one of such rules. This means that, in line with internal Parliamentary procedure, each Bill should be adopted by the Sejm in a transparent manner, whereas open access to such procedure may only be denied for the good of the State.

The beginnings of cyber defence date back to the creation of the Internet, and the assumptions behind it, involving the improvement in the capacity of US military computer networks to provide better protection against nuclear attacks. Afterwards, the assumptions behind cyber defence included combat

⁹ Decree of the Constitutional Tribunal of 23 March 2006, Case File No. K 4/06, OTK-A 2006, No. 3, item. 32.

¹⁰ Articles 21–25, Chapter 5 “The obligations of public authorities” of the National Cybersecurity System Act of 5 July 2018 (Journal of Laws of 2018, item 1560, as amended).

information and information operations¹¹. The date which marks the symbolic beginning of the Internet in Poland is 17 August 1991. This was most probably the day on which the first email was sent from Poland to Copenhagen with the use of the TCP/PI protocol¹².

In past decades we have all witnessed the great success of the network, and in recent years the Internet has become an integral part of our lives. Along with the emergence of the Internet, Parliamentary services have developed a platform on which the full legislative process is published, and there is a special search engine which includes information uploaded onto the archives about the earlier terms of office. Users have access to Bills, Statements of Reasons, the work of committees, and stenographic reports, as well as the Journal of Laws, in which Acts are published. The negative consequence of legislative proceedings' being on the Internet is access by persons to whom such a service is not intended. The plethora of data and information available on Parliament's website requires services to apply all available safeguards which facilitate the maintenance of the published content in their original form. To this end, all possible safeguards, site parameters, and sets of results are used. The software which is operated by users reflects the directly formulated parameters characterising a given user who connects to the network with the use of such software. While the legislative process shown on the website is available to the public, the initial phase of internal working on amendments is classified¹³. This results from the fact that the amendments to Bills must first be uploaded onto the system and checked by the services of the Chancellery of the Sejm before they are published on the website. Such restrictions are a consequence of the fact that certain additional criteria in the process of passing an Act have accumulated. While searching for, or generating, information by automated means, recipients can follow the legislative process in the form of video broadcasts.

All types of attack constitute a clear threat to the correctness of the legislative process, and to files uploaded onto the website, due to the disruption

11 R. Lelito, *Podstawy cyberbronności państwa*, [in:] *Wojskowe systemy łączności w systemie bezpieczeństwa państwa: wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, red. B. Biernacik, G. Pilarski, Warszawa 2018, p. 100.

12 R. Balicki, *Demokracja w czasie Internetu*, [in:] *Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, red. R. Balicki, M. Jabłoński, Wrocław 2018, p. 348.

13 P. Chybalski, *Poprawka w postępowaniu ustawodawczym w świetle Konstytucji RP*, Warszawa 2014, p. 223 et seq.

of information transfer as part of the public debate. It is vital to apply a reliable firewall preventing unauthorised third-party access, separating the legislative process from potential impact, i.e. from altering files and their content. This phenomenon can also demonstrate certain irregularities, or mislead citizens and services. Such form of media misinformation can be the outcome of deception or a game being played by people who do not realise, or are not aware of the fact that, their actions are disrupting the work of Parliament.

Such activities often take the form of an extraordinary Internet “warfare” which results in the exerting of influence on the shape of the most important process in the country. Without doubt, this also affects the course of procedures and the occurrence of potential errors, as well as the outcome of legislative process in its final form.

We cannot imagine our lives without the new technologies which have a significant influence on public access to the legislative process. They have become an inseparable part of Parliament’s operations which we can witness on a daily basis. They not only assist legislative work in the Parliament, but also co-create the legal, and, for many people, the political, spheres of the country¹⁴. If we wish the system to work properly, it is necessary to adopt numerous diverse measures in the field of the legislative process which enable people to identify false information. The operations of services in charge of data protection should be managed with care, and we should exercise the utmost caution. The Internet should be seen as an invention which not only serves educational purposes but as a source of threats arising from various types of attack.

The situation is similar in the case of national cyber defence, including the protection of the legislative process in the Parliament when affected by the ICT “maelstrom”, including the Internet. If the State defence system is part of the security domain, cyber defence should be treated as an element in our cybersecurity system. The cyber defence of the legislative process should be understood as preparing ICT systems (networks) and the data processed in such systems, critical from the point of view of Parliamentary interests, for protection against attacks. The key role in cybersecurity has been assigned to services which should have the capacity to protect their own ICT systems

¹⁴ R. Zięba, *Teoria bezpieczeństwa państwa w ujęciu neorealistycznym*, [in:] *Teoretyczne i praktyczne aspekty bezpieczeństwa państwa*, red. G. Gasztold, M. Brzeziński, Warszawa 2018, p. 13 et seq.

and the resources accumulated on them, and active defence and offensive capabilities in the cyberspace.

It should be stressed that the notions of legal security and legal certainty are of great significance here¹⁵. On the one hand, legal certainty arises from the application of the law, while on the other hand it means that the legal security of the legislative process must be ensured in all respects¹⁶. The list of measures aimed at providing the security of the legislative process must be subject to close surveillance¹⁷. In the context of the above discussion, it can be stated that every breach affecting information components resulting in their unfitness for a given purpose constitutes a threat to the open access to the legislative process. Hence the list of threats to public access to the legislative process is extremely long. What's more, due to the extensive development of information technologies, any attempt to create an exhaustive catalogue of such threats must be doomed to failure, as every innovative and ground-breaking technology which is crucial to the transfer and processing of information results in new types of threat, including risks to the legislative process. The development of the Internet, as a widely available communication platform characterised by interactivity, i.e. providing not only access to information, but also the possibility to create and disseminate content, can serve as an example here.

Generally speaking, the basic threats to the information security of the legislative process include 1) no access to legislative information, 2) excessive legislative information, 3) access to false information and legislative misinformation, 4) no protection of own legislative information resources, 5) no control over legislative information-transfer channels.

Some threats are objective, while others are a consequence of vulnerabilities in legislative bodies and their internal structures. It is difficult to reduce the quantity of information in a democratic society, just as it is not possible to exercise full control over all IT-related activities, which could end in censorship.

15 M. Jurgilewicz, *Rzecz o bezpieczeństwie prawnym*, [in:] *W kręgu nauki o bezpieczeństwie...*, p. 30 et seq.

16 M. Leszczyński, *Od bezpieczeństwa państwa do bezpieczeństwa jednostki. Ewolucja w podejściu do badań bezpieczeństwa*, [in:] *Współczesne wyzwania państwa i prawa: księga jubileuszowa z okazji 45-lecia pracy naukowej Profesora Jerzego Jaskierni*, red. Ł. Baratyński, P. Ramiączek, K. Spryszak, Toruń 2017, p. 560.

17 M. Leszczyński, *Istota systemu bezpieczeństwa państwa*, [in:] *Bezpieczeństwo społeczne a bezpieczeństwo państwa*, Kielce 2009, p. 21 et seq.

On the other hand, the lack of access to information on the legislative process might be the outcome of poor performance by the services in charge of security. In turn, the failure to provide proper safeguards might result in the fact that the State will no longer have the capacity to keep confidential those pieces of information which should be hidden from potential opponents. Finally, the inability to counteract hostile misinformation campaigns via the Internet can be regarded as a weakness of the State.

The basic threats to the security of the legislative process include 1) the unauthorised disclosure of legislative information, which can be the outcome of an error, or be dictated by political or economic premises, 2) the breach of civil rights by authorities (the restriction of public access to the legislative process), 3) the operations of groups intentionally manipulating the flow of legislative information, 4) computer crime, 5) information combat aimed at obtaining legislative information, 6) legislative-information espionage.

In classifying internal threats to the legislative process we can divide them into threats related to the imperfect functioning of civic society, threats related to the functioning of cyberspace and mass-media space, and those regarding the use of sensitive issues in international relations¹⁸.

The next issue involves the presence of a legislative-information deficit in a society, which in turn makes the public vulnerable to misinformation, and facilitates the operations pursued by agents of influence.

Threats in cyberspace, including misinformation, should be considered as a category of risks especially germane to the legislative process. Hostile propaganda, attacks can result in the disruption of ICT systems, the existence of technology gaps affecting the legislative process which provide an opportunity to interfere, often in an unnoticeable way, in the content of Bills or Acts, and affecting the capacity to act in the cyberspace.

In addition, due to the presence of the Republic of Poland in the global cyberspace, cybernetic attacks can occur which in fact can shape the legislative process or hinder the flow of legislative information from the Parliament.

Unwanted, external information which can impact on data impinging on legislative procedures, in the form of IT attacks aimed at controlling the decision-making processes of Parliament, should be considered as a serious threat.

¹⁸ A. Rzepka, *Bezpieczeństwo międzynarodowe w dobie globalizacji*, [in:] *Bezpieczeństwo XXI wieku: szanse - zagrożenia - perspektywy: aspekty prawne*, red. T. Gadkowski, Poznań 2018, p. 156 et seq.

The dependence of contemporary Parliaments on efficient systems of processing and distributing legislative information is a fact. The notion of legislative-information security should be understood in its broad sense, with its objective scope covering the capacity to provide legislative information, analyse, disseminate and protect own legislative information resources, and the ability to identify and counteract hostile IT operations aimed at exerting influence on the legislative process. In particular, this refers to information in cyberspace.

Therefore, the notion of legislative-process security is closely linked to information combat, i.e. the combat in which legislative information can be both a weapon and the target of attacks. It requires the protection of own legislative-information resources and legislative-information systems, and the ability to perform own information operations and misinformation campaigns. Threats to legislative-information security are related to information components, as their breach can result in incomplete and inaccurate information which is not fit for its purpose.

The preparation of an Act is a complex and long-lasting process. However, some proceedings require fast decision-making, with insufficient time for analysing the legislative information entered in the system. As a result, accelerating the performance of tasks in Parliament IT systems can facilitate unauthorised access to information and its alteration. Also, with rapid technological advancements in recent years, the meaning of cyberspace has evolved considerably. At present it is most of all virtual space where network-connected computers and other digital media (mobile phones, tablets, radio, televisions) communicate, and where Parliamentary activities have also found their place. The protection of cyberspace has become one of the most frequently discussed issues related to the security of the legislative process. In short, the course of the legislative process needs to be organised in this Internet space. It is necessary to modify, supplement, or develop security mechanisms for the security of the legislative process.

Given the above, as regards the security of the legislative process on the Internet, the Republic of Poland is obligated to generate the country's minimum required capacities by establishing legislative procedures for the security of network and information systems¹⁹. It seems a positive thing that

¹⁹ P. Kościelny, *Opinia prawna z dnia 4 czerwca 2018 r. do rządowego projektu ustawy o krajowym systemie cyberbezpieczeństwa*, Sejm document No. 2505, The Analysis Department at the Chancellery of the Sejm, p. 2.

Poland has established a structured cybersecurity threat-management model, in such a way that it is focused on capacity-building within the scope of ongoing threat monitoring and integrated cybersecurity management at the national level, and the protection of security and public access to the legislative process have been properly incorporated into the system.

Bibliography

- Balicki R., *Demokracja w czasie Internetu*, [in:] *Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, red. R. Balicki, M. Jabłoński, Wrocław 2018.
- Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.
- Chybalski P., *Poprawka w postępowaniu ustawodawczym w świetle Konstytucji RP*, Warszawa 2014.
- Garlicki L., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 2, Warszawa 2001.
- Jaskiernia J., *Zasady demokratycznego państwa prawnego w sejmowym postępowaniu ustawodawczym*, Warszawa 1999.
- Jurgilewicz M., *Rzecz o bezpieczeństwie prawnym*, [in:] *W kręgu nauki o bezpieczeństwie*, red. M. Jurgilewicz, S. Sułowski, Warszawa 2018.
- Lelito R., *Podstawy cyberobronności państwa*, [in:] *Wojskowe systemy łączności w systemie bezpieczeństwa państwa: wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, red. B. Biernacik, G. Pilarski, Warsaw 2018.
- Leszczyński M., *Istota systemu bezpieczeństwa państwa*, [in:] *Bezpieczeństwo społeczne a bezpieczeństwo państwa*, Kielce 2009.
- Leszczyński M., *Od bezpieczeństwa państwa do bezpieczeństwa jednostki. Ewolucja w podejściu do badań bezpieczeństwa*, [in:] *Współczesne wyzwania państwa i prawa: księga jubileuszowa z okazji 45-lecia pracy naukowej Profesora Jerzego Jaskierni*, red. Ł. Baratyński, P. Ramiączek, K. Spryszak, Toruń 2017.
- Leszczyński M., *Spółczeństwo „zatomizowane” jako skutek rozpadu tradycyjnych wspólnot. Implikacje dla współczesnego bezpieczeństwa*, [in:] *Prawne, instytucjonalne i społeczne uwarunkowania bezpieczeństwa*, red. S. Bębas, A. Gołębiowski, Radom 2014.
- Letkiewicz A., *Istota współczesnego zarządzania jako element bezpieczeństwa*, [in:] *W kręgu nauki o bezpieczeństwie*, red. M. Jurgilewicz, S. Sulowski, Warszawa 2018.
- Rzepka A., *Bezpieczeństwo międzynarodowe w dobie globalizacji*, [in:] *Bezpieczeństwo XXI wieku: szanse – zagrożenia – perspektywy: aspekty prawne*, red. T. Gadkowski, Poznań 2018.
- Stębel M., *Rola polskiego parlamentu po transformacji ustrojowej*, [in:] *XV lat obowiązywania Konstytucji z 1997 r. Księga jubileuszowa dedykowana Zdzisławowi Jaroszowi*, red. M. Zubik, Warszawa 2012.
- Szepietowska B., *Proces ustawodawczy*, [in:] *Parlament model konstytucyjny a praktyka ustrojowa*, red. Z. Jarosz, Warszawa 2006.
- Zięba R., *Teoria bezpieczeństwa państwa w ujęciu neorealistycznym*, [in:] *Teoretyczne i praktyczne aspekty bezpieczeństwa państwa*, red. G. Gasztold, M. Brzeziński, Warszawa 2018.

Cyberprzestrzeń a jawność procesu ustawodawczego

Streszczenie

Jawność procesu legislacyjnego jest jedną z zasad prawa parlamentarnego. Jawność procesu legislacyjnego to przede wszystkim jawność debaty, jawność przedkładanych wniosków i przedłożeń, jawność głosowania, jawność podejmowania uchwał oraz jawność dokumentów stanowiących podstawę do obrad Sejmu. Społeczeństwo dzięki nowoczesnym środkom przekazu i bezpośrednim transmisjom ma dostęp do pełnych obrad parlamentu i procesu legislacyjnego. Odbiorca, wyszukując informacji bądź podczas jej automatycznego generowania, może śledzić proces ustawodawczy w formie wideo. Wszelkiego rodzaju internetowe ataki stanowią oczywiste zagrożenie prawidłowości procesu ustawodawczego i mogą prowadzić do zaburzenia procesu przekazywania informacji w ramach debaty publicznej.

Słowa kluczowe: proces legislacyjny, zasada jawności, prawo parlamentarne, cyberprzestrzeń, informacja legislacyjna