

Paulina Korycińska-Rządca

University of Białystok, Poland

p.korycinska@uwb.edu.pl

ORDIC ID: <https://orcid.org/0000-0002-6177-7409>

Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets against Unauthorised Acquisition, Use and Disclosure by Its Employees?

Abstract: One of the natural consequences of the development of technology is that an entrepreneur's confidential information, including trade secrets, is commonly stored in electronic files. This form of information storage inevitably entails challenges in the area of its protection. The coronavirus pandemic has drastically accelerated the process of dissemination of new models of employment, in particular remote (distance) work and cloud working, and has made the protection of an entrepreneur's secrets against unauthorised use even more complicated. This is due to the fact that in such models of employment, employees obtain access to their employer's data remotely, which may decrease the employer's level of control. To remedy this, employers may undertake various steps aimed at ensuring that their secrets are well protected; however, such actions may affect the free movement and mobility of workers. The purpose of this article is to verify how, in these circumstances, the measures provided for in EU law face the challenges of protecting an employer's secrets against unauthorised use by employees and how they define the scope to which they can be applied without the abuse of employees' rights and unjustified restrictions on their mobility. For that purpose, the author analyses in particular Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against Their Unlawful Acquisition, Use and Disclosure. This research is based mainly on the dogmatic method of analysis.

Keywords: Directive (EU) 2016/943, employees, employment relationship, trade secrets

Introduction

Confidential information, including trade secrets, is a determining factor as regards competitiveness and innovation-related performance in the market. The summary of responses gained by the European Commission in the course of a public consultation on protection against the misappropriation of trade secrets and confidential business information, launched on 11 December 2012 and closed on 8 March 2013, shows that 65% of companies that participated see a strong positive influence for trade secrets in the areas of, amongst others, research and development, the exploitation of innovation, and the innovative and competitive performance of SMEs (European Commission, 2012, p. 3). Interestingly, as many as 53% of respondents indicated that the most typical perpetrators of trade secret misappropriation were former employees (European Commission, 2012, p. 13).

The fact that so many respondents considered departing employees to be the biggest threat to trade secrets should not, however, be a surprise. Employees get access every day to various types of their employer's data, including trade secrets and other confidential information. Such access is a natural consequence of the employment relationship, as it would be irrational if the employer denied the employee information necessary to perform certain tasks but still required the job to be done properly. If the employer decides to provide an employee with information that is necessary for the proper performance of their entrusted duties, such sharing can be defined as intentional. Simultaneously, the employee may also get access to data that are not necessary for him/her to perform his/her assigned duties; this may happen by accident (e.g. if the data were in a message that was sent to him/her accidentally), as a consequence of faulty protection of data (e.g. when the employee uses an opportunity to see data that were improperly protected against unauthorised access) and as a result of a breach of the duty of confidentiality.

Recently the protection of employers' confidential information has become even more challenging. The reason for this, amongst others, is connected to the two factors. First of all, as a result of the development of technology, an entrepreneur's data are more and more commonly stored in electronic files. This form of information storage inevitably entails challenges in the area of its protection. Secondly, the coronavirus pandemic has drastically accelerated the process of dissemination of new models of employment, in particular remote (distance) work and cloud working; this has made the protection of entrepreneurs' secrets against unauthorised use even more complicated, because in these models of employment, employees obtain access to their employer's data remotely, which may decrease the employer's level of control.

The key EU legal act which deals with the issue of entrepreneurs' confidential information is Directive (EU) 2016/943 of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against Their Unlawful Acquisition, Use and Disclosure, which was adopted on

8 June 2016 and had to be transposed by EU Member States by 9 June 2018. It is binding not only on EU Member States but also on Iceland, Lichtenstein and Norway, as it was included in the European Economic Area (EEA) Agreement by Decision 91/2019 of 29 March 2019. Directive (EU) 2016/943 harmonised in many ways issues connected to trade secrets protection. However, it does not contain any specific rules dedicated solely to the protection of trade secrets gained by an employee in connection with employment relationship. Nevertheless, its preamble proves that EU legislatures were aware of possible conflicts between a legitimate interest in the protection of an employer's confidential information (freedom of establishment) and employees' legitimate interests in being able to change jobs (free movement and mobility of workers). The need to show 'special diligence' in cases concerning labour mobility has also been stressed by the European Court of Human Rights (Judgment of the European Court of Human Rights 2006, para. 42).

The purpose of this article is to verify how, in these circumstances, the measures provided for in EU law face the challenges of protecting an employer's secrets against unauthorised use by employees, and how they define the scope to which they can be applied without the abuse of employees' rights and unjustified restrictions on their mobility. For that purpose, the author analyses Directive (EU) 2016/943 in particular. The research is based mainly on the dogmatic method of analysis.

1. The definition of trade secrets in Directive (EU) 2016/943

Directive (EU) 2016/943, in its Article 2(1), defines a 'trade secret' as information which meets all of the following requirements:

- a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- b) it has commercial value because it is secret;
- c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.¹

In accordance with Directive (EU) 2016/943, the requirement of secrecy shall be understood in a way that information shall not be generally known amongst or readily accessible to persons within the circles that normally deal with the kind of information in question. Article 2(1)(a) of the Directive also emphasises that a single piece

1 These requirements recall the criteria of 'undisclosed information' contained in Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement); the wording of them is identical (at least in the English versions).

of information, as well as the precise configuration and assembly of its components, may constitute a trade secret.

Directive (EU) 2016/943 attaches commercial value to the confidential nature of information in question. It requires that information shall have commercial value due to the fact that it is secret. It should be noted that this requirement has not been transposed by the EU Member States uniformly: there are countries that copied this criterion from the Directive and require that information has to have commercial value resulting from its secret nature, and countries where the requirement of commercial value is not linked to the confidentiality of information (e.g. Poland²). Such an approach taken by national legislatures shall not be deemed as contrary to the Directive, due to fact that this legal act sets a minimum standard, from which EU Member States can deviate to incorporate stricter measures (minimum harmonisation).

The assessment of whether information has economic value should be made using objective criteria. In particular, the mere belief of an undertaking that particular information has economic value does not constitute sufficient basis for it to be protected as a trade secret (Du Vall & Nowińska, 2013, p. 198; Korus, 2002; Korycińska-Rządca, 2020, p. 132; Michalak, 2016, p. 402; Nowińska, 2018, p. 233). Simultaneously, the concept of economic value should be interpreted liberally in order to allow for it to include information having at least minimal economic value (Korycińska-Rządca, 2020, p. 132).

An undertaking that wishes to protect information as a trade secret has the greatest impact on the fulfilment of the last condition, i.e. the requirement of taking reasonable steps to keep information secret. In fact, the burden of meeting this condition rests entirely with the undertaking that holds the trade secret. In Poland, the threshold established in case law in this regard is relatively low, as courts usually assume that any actions which demonstrate that the information is confidential is enough and that, in specific circumstances, the obligation to maintain secrecy may be determined by the nature of the information itself, combined with the level of professional knowledge of the persons who came into possession of it (Judgment of the Supreme Administrative Court 2023). In the literature, it is emphasised that taking actions to maintain confidentiality of information is not only aimed at meeting the requirement of secrecy but also demonstrates the undertakings' will for the information to be protected as a business secret (Będkowski-Kozioł, 2014, pp. 208–209). This requirement can be considered from two aspects: in relation to the undertaking's employees and in relation to third parties. In relation to employees, the employer shall inform those who have access to the information about its secret nature, as well as taking appropriate organisational actions to keep it secret (Sołtysiński & Gogulski,

2 In accordance with Article 11(2) of the Act of 16 April 1993 on Combating Unfair Competition, '[a] trade secret shall mean technical, technological, organisational information or other information of economic value.'

2019, pp. 443–445), in particular limiting access only to a narrow circle of employees, obliging employees who have access to such information to maintain confidentiality, introducing access control to rooms where documents containing trade secrets are kept, limiting access to such information located on computers and monitoring or establishing other technical safeguards (Będkowski-Kozioł, 2014, pp. 208–209; du Vall & Nowińska, 2013, pp. 190–191). The actions taken in relation to third parties may include concluding confidentiality agreements or appropriate marking of disclosed materials containing confidential information (Będkowski-Kozioł, 2014, pp. 208–209; Sołtysiński & Gogulski, 2019, p. 444). The assessment of this requirement should be made taking into account the circumstances of the specific case, such as the size of the enterprise (Sołtysiński & Gogulski, 2019, pp. 444–445; see also Michalak, 2006, pp. 131–132; Wojcieszko-Głuszko, 2002, p. 74 ff.), the character of the secret data, the economic purpose of the legal transaction, the circumstances surrounding the contract and the principles of social coexistence or customs (Sołtysiński & Gogulski, 2019, p. 444; Traple, 2003, p. 8).

Article 2(1) of Directive (EU) 2016/943 does not give any example of information that may be a trade secret. Irgens-Jensen (2023, pp. 501–509) rightly points out that the Directive's threshold for information to qualify as a trade secret is low. In practice, a trade secret may include information of very different natures, amongst others:

- undisclosed know-how and business information;³
- technological information;⁴
- ideas, plans and concepts;
- the result of marketing research;
- the composition of the product;
- the name, price and date of sale of the product or a list of customers,

provided, however, that such information meets all three requirements stipulated in Article 2(1) of the Directive (EU) 2016/943 (on the meaning of trade secrets by national courts, see Irgens-Jensen, 2023, pp. 501–509).

2. The distinction between 'trade secrets' and 'skills and knowledge'

The broad understanding of 'trade secret' ensures the protection of a wide range of information, the confidentiality of which is important for the competitiveness and innovation-related performance of the undertaking who holds the secret. In this sense it ensures freedom of establishment as well as protection of the employ-

3 This can be implied from the title of Directive (EU) 2016/943 as well as from motive 14 of its preamble.

4 This can be implied from motive 14 of the preamble to Directive (EU) 2016/943.

er's right to privacy, which is safeguarded under Article 8 of European Convention on Human Rights signed in Rome on 4 November 1950 (on the issue of protection of entrepreneurs' rights, see Wiśniewski, 2023, pp. 11–33). Simultaneously, such an approach may hinder the free movement and mobility of workers, as employees may be afraid that their skills and knowledge learned during their employment constitute trade secrets which they will not in fact be able to lawfully use anywhere else, because it is unlikely that they will obtain the employer's consent to do so (Irgens-Jensen, 2023, p. 509).

The EU legislature was clearly aware that the protection of trade secrets required by Directive (EU) 2016/943 may lead to collision between freedom of establishment and the free movement and mobility of workers (see recital 13 of the preamble). In recital 14 of the preamble to the Directive, it is indicated that the definition of 'trade secret' excludes, amongst other things, the experience and skills gained by employees in the normal course of their employment. This distinction, however, is not explicitly repeated in the definition of 'trade secret' contained in Article 2(1). In the literature, it is emphasised that experience and skills are inseparable from the employee (Kolasa, 2018, p. 77) and that they cannot be recorded or disclosed to another entity in the form of a description, plan or drawing (Sołtysiński & Gogulski, 2019, p. 436 ff.). Consequently, it is indicated that experience and skills do not constitute 'information' as indicated in Article 2(1), and therefore they cannot be qualified as a trade secret (Domeij, 2020, p. 166; Kolasa, 2018, p. 77).

The intention of EU legislation to exclude employees' experience and skills gained during their employment from the definition of a trade secret is clear. It is also supported by Article 1(3)(b) of Directive (EU) 2016/943, which states that the Directive shall not offer any ground for limiting employees' use of experience and skills honestly acquired in the normal course of their employment. Interestingly, in Sweden the distinction between trade secrets and skills and experience, as provided for in recital 14 of the preamble to Directive (EU) 2016/943, has been explicitly expressed in Section 2(2) of the Act on Trade Secrets (SFS 2018:558), whereas other EU Member States have decided not to include such a distinction directly in the provisions of law.

The literature emphasises that in the process of assessing whether the 'information' in question constitutes a trade secret or the individual experience and skills of the employee, it may be helpful to take into account not only the character of the information but also such factors as whether the information is recorded in the form of a document or electronic file, whether is only in the employee's mind or whether it is possible to identify the information and carve it out from the individual experience and knowledge of the employee (Sołtysiński & Gogulski, 2019, pp. 443–445). It might also be useful to take into consideration the employee's position, as the scope of confidentiality obligations is often wider in the case of technical and research and development staff than for technicians or engineers in production de-

partments (also see the Judgment of the Court of Appeal in Kraków 2013; Michalak, 2006, p. 83; Wojcieszko-Głuszko, 2002, p. 133 ff.). Nevertheless, drawing a clear line between what is undisclosed know-how and what constitutes the individual experience and skills of the employee may be very difficult in practice (Sołtysiński & Gogulski, 2019, p. 436 ff.).

The practical difficulties with making a distinction between a trade secret and the experience and skills of the employee have led to differences in the approaches of national courts in different jurisdictions as to the manner by which they safeguard the interests of employees in dispute with their employers, who claim that the use of certain information obtained by the employees in the course of their employment was unlawful. National courts in some EU Member States (e.g. Poland), despite the existing practical difficulties, follow the approach supported by the wording of the Directive that the individual experience and skills of employees are excluded from the definition of 'trade secret' and as such are not protected as a trade secret. Consequently, they focus on the distinction between trade secrets and the experience and skills gained by employees in the normal course of employment. Nevertheless, analysis of the jurisprudence indicates that it is very difficult to assess whether information constitutes a trade secret or the employee's experience and skills. In other EU Member States (e.g. Germany, France and Sweden), national courts assume that such a distinction between these categories is almost impossible to draw, and instead of making attempts to do so they focus on the weighing of interests (see Ir gens-Jensen, 2023, p. 510). Regardless of the approach, the assessment of whether the employee may use certain information for purposes other than their job within the employment relationship in connection with which it was gained is difficult and is subject to a high risk of error. This risk may be even higher if the employee is the one to make the assessment on his/her own, as s/he may not have full knowledge of the importance of the information. At the same time, any mistakes in the assessment process which result in unlawful use of a trade secret by the employee are to be borne by them. At least some of the difficulties in this area may be solved by signing a confidentiality agreement stipulating precisely which information constitute the employer's secrets.

3. Lawful and unlawful acquisition of trade secrets by the employee

In accordance with Directive (EU) 2016/943, the acquisition of a trade secret shall be considered lawful, in particular, when the trade secret is obtained by any practice⁵ which, under the circumstances, is in conformity with honest commercial practices (Article 3(1)(d)) and to the extent that such acquisition is required or al-

5 Other than those expressly stipulated in Article 3(1)(a)–(c) of the Directive.

lowed by EU or national law (Article 3(2)). In Articles 4(2) and 4(4), the Directive stipulates circumstances under which the acquisition of a trade secret shall be considered unlawful. These provisions state the rules that shall be applicable, regardless of who the acquirer of trade secret is. The Directive does not oblige EU Member States to provide for any special rules applicable for the assessment of whether an acquisition of the employer's trade secret by an employee was lawful. Therefore, the acquisition of the trade secret by the employee shall be considered unlawful in the following situations:

- if the trade secret was acquired by the employee without the consent of the employer who is the holder of the trade secret, whenever such acquisition is carried out by unauthorised access to, appropriation of or copying of any data carrier containing the trade secret or from which the trade secret can be deduced, provided that this data carrier is lawfully under control of the employer;
- if the trade secret was acquired by the employee without the consent of the employer through any other conduct which, under the circumstances, is considered contrary to honest commercial practices (Article 4(2) of the Directive);
- if the employee at the time of the acquisition knew or, under the circumstances, ought to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

From these provisions it can be implied that whenever an employee acquires an employer's trade secrets with the latter's consent, the acquisition shall be considered lawful. Such consent can be both express or implied (i.e. when access to certain trade secrets is justified due to the position held by the employee or duties assigned to him/her).

Undoubtedly, one of the challenges connected to the employment relationship is the protection of confidential information against unauthorised acquisition by employees. It should be taken into consideration that an employee who is a part of the employer's organisation may have an opportunity to get access to certain data more easily than a third party. To ensure that information is protected as a trade secret, the employer shall take reasonable steps to reduce the risk of unjustified acquisition of the secrets by an employee (i.e. acquisition of the secrets on the occasion of an employment relationship). As was indicated above, taking such steps is crucial for fulfilling the requirements of being a trade secret. These actions may be challenging, especially when the employer's database is electronic and available for employees remotely. The fact that an employee who should not have access to certain information is able to obtain it may rise doubts as to whether such information constitutes a trade secret within the meaning of Article 2(1) of Directive (EU) 2016/943.

However, it shall not *prima facie* mean that such information is not a trade secret. Polish case law proves that such assessment is made on a case-by-case basis. For example, the Supreme Court has classified transferring the employer's documents from its server to the employee's private email as a violation of basic employee obligations arising, amongst other things, from the rules protecting trade secrets and not as a circumstance that constitutes an obstacle to recognising the information in question as not being a trade secret (Judgment of the Polish Supreme Court 2019).

The general circumstances stipulated in the Directive under which the acquisition of a trade secret is considered unlawful are broad enough to cover situations whenever an employee, through his/her actions, gains access to trade secrets that s/he should not have access to, in particular if such acquisition is carried out without the employer's express (or implied, i.e. resulting from the position held or assigned duties) consent or even his/her knowledge.

4. Lawful and unlawful use and disclosure of trade secrets by the employee

In accordance with Article 3(2)(d) of Directive (EU) 2016/943, the use or disclosure of a trade secret shall be considered lawful to the extent that such use or disclosure is required or allowed by EU or national law. The Directive does not oblige EU Member States to provide for any special rules applicable for the assessment of whether an employee's (or ex-employee's) use or disclosure of their employer's (or former employer's) trade secret was lawful. In accordance with the requirements of this Directive, the use or disclosure of the employer's trade secret by the employee (or ex-employee) shall be considered unlawful in the following situations:

- if such a trade secret has been acquired by the employee (or ex-employee) unlawfully (Article 4(3)(a) of the Directive);
- if the employee (or ex-employee) has broken their duty not to use or limit the use of the trade secret, regardless of the source of such an obligation (i.e. whether it is a contractual obligation or an obligation arising from law) (Article 4(3)(b)–(c) of the Directive);
- if the employee (or ex-employee), at the time of the acquisition, use or disclosure, knew or, under the circumstances, ought to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully (Article 4(4) of the Directive).

Consequently, it is implied that, in accordance with the approach taken by the Directive, whenever an employee uses or discloses their employer's trade secrets in connection with the employment relationship and for the sole purpose of performing their assigned duties properly, such use or disclosure shall be considered lawful. The same relates to a situation in which the employee (or ex-employee) uses a trade

secret for other purposes or discloses it to any third party with the employer's consent.

On the contrary, if the employee obtained the trade secret lawfully in connection with the employment relationship, the assessment of whether the subsequent use of such a secret was lawful depends on the fact of whether this former employee, at the time of the use of it, was bound by a confidentiality agreement or any other duty not to disclose the trade secret or limit the use of it. The Directive does not, however, stipulate when such other duty may exist nor how long it applies. An analysis indicates that EU Member States have not addressed this shortcoming of the Directive uniformly. On the one hand, there are countries like Germany and the Scandinavian countries where the courts establish, on a case-by-case basis, an implied duty of confidence, provided, however, that a weighing-up of interests favours the employer (see Irgens-Jensen, 2023, p. 499). On the other, in the case of Poland, an employee is under a statutory obligation to keep any information secret if the disclosure of it could expose the employer to harm (Article 100(2)(4), Labour Code 1974). This obligation is not limited only to trade secrets within the meaning of the Directive but goes far beyond. A similar approach is also taken in English and American jurisprudence (cf. Sołtysiński & Gogulski, 2019, p. 454 ff. as well as the literature indicated therein). Interestingly, in Poland, before the transposition of the Directive, it clearly resulted from the law that the employee was under an obligation not to transfer, use or disclose a trade secret during their employment and for a period of three years from the termination of the employment relationship, unless the contract provided otherwise or a state of secrecy ceased (Article 11(2), Act on Combating Unfair Competition 1993 in the wording in force till 4.9.2018). Although the rule expressly indicating the length of the former employee's duty of confidentiality was convenient – especially from the employee's perspective – it was not in line with the Directive and therefore was repealed. Due to this, it is recommended that the scope of the duty of confidentiality is established in a non-disclosure agreement signed by employer and employee (Nowińska, 2022, p. 261). Nevertheless, even if the parties conclude such an agreement, the provisions of it may be controlled by a court in proceedings regarding claims arising from an alleged breach of the duty of confidentiality. In such proceedings the court shall carry out an examination on a case-by-case basis, particularly if the contractual obligation of the former employee did not restrict their mobility.

5. Protection of trade secrets v. the mobility of workers

Article 6(1) of the Directive obliges EU Member States to provide for the measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets. In accordance

with Article 7(1), they shall be applied in a manner that is proportionate, avoids the creation of barriers to legitimate trade in the internal market and provides for safeguards against their abuse. Such measures, procedures and remedies shall also be provided for against an employee (or ex-employee) who has unlawfully acquired, used or disclosed the secrets of his/her employer (or ex-employer) and should allow the employer to obtain redress for the unlawful acquisition, use or disclosure of their secret. Simultaneously, the Directive imposes on EU Member States an obligation to ensure that competent judicial authorities may, upon the request of the respondent, apply appropriate measures where an application concerning the unlawful acquisition, use or disclosure of a trade secret is manifestly unfounded and the applicant is found to have initiated the legal proceedings abusively or in bad faith (Article 7(2) of the Directive). This solution may be seen as protection of the employee (or ex-employee) against initiation of proceedings abusively or in bad faith.

Conclusions

The analysis contained in this paper leads to the conclusion that the Directive obliges EU Member States to provide for measures, procedures and remedies in order to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets. The requirements for these measures, procedures and remedies are generally common, regardless of who the trade secrets' holder is and who acquires, uses or discloses them. Although the Directive highlights the potential conflict between the employer's interests and the mobility of workers, and expresses the EU legislature's intention to exclude the individual experience and skills gained by employees in the normal course of their employment from protection as a trade secret, the only real difference made in the Directive in the cases regarding the protection of trade secrets in connection to an employment relationship is that the Directive enables EU Member States to limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of an employer's trade secret where they act without intent (Article 14(1) of the Directive).

What can be assessed positively is the fact that the Directive obliges EU Member States to ensure that a respondent is able to request a competent judicial authority to apply appropriate measures in cases where an application concerning the unlawful acquisition, use or disclosure of a trade secret is manifestly unfounded and the applicant is found to have initiated the legal proceedings abusively or in bad faith. This may be an important tool to prevent employers attempting to use measures and legal procedures adopted to protect trade secrets as a threat, in order to force an employee not to change their job or to prevent a former employee from using their skills and knowledge gained in the normal course of employment somewhere else.

Simultaneously, the analysis indicates that there are challenges and difficulties with the protection of trade secrets in connection to the employment relationship for both parties. From the employer's perspective, the roots of potential difficulties with the protection of trade secrets in connection with the employment relationship is that the model of the protection of trade secrets required by the Directive is based on the assumption that the owner of a trade secret shall manifest his/her intention to maintain the secrecy of information that s/he wishes to be protected as a trade secret by his/her actions. Consequently, the burden of taking reasonable protective steps is carried by the owner of the trade secret – in this case by the employer. This means that the employer shall identify the potential risks connected to the protection of the secret in the organisation and shall take reasonable steps (e.g. organisational and technological) to minimise the risk that secrets will be acquired by those employees that do not need them, as well as to make sure that employees who have access to the secrets are aware of their confidential nature and that they know exactly which information may or may not be disclosed. Any omissions in this regard may result in a refusal to protect the employer's information as a trade secret.

From the employee's perspective, the main difficulties are connected with the practical difficulties in drawing a line between what is a trade secret and what are individual experience and skills. It should be taken into consideration that any mistakes in the assessment in this regard which lead to the unlawful use of a trade secret are to be borne by the employee. The approach taken by the national courts of some EU Member States, concentrating on weighing the interests of the employer and employee rather than on making this distinction in practice, is an interesting way of combating this problem. However, a state of uncertainty remains on the employee's side as to the possibility of using certain information.

Taking into consideration the complexity of the issues connected to trade secrets, it is doubtful whether it would be possible to remove these difficulties through legislative changes. It seems that the existing shortcomings of the Directive in this regard are being addressed by national case law. This method is, however, subject to the risk of discrepancies between the approaches taken in different countries. The simplest solution to combating or at least reducing these shortcomings, especially in connection to the employment relationship, could be a confidentiality agreement signed between the employer and the employee, which precisely stipulates what information, in the case of the particular employer, is a trade secret, what actions connected to such information shall be taken by the employee (in particular how the employee shall protect the information and how and when s/he can use or disclose it) and what actions are forbidden. Such an agreement could be amended, if needed. The practice of signing such agreements could also be helpful for employers in the process of proving that they took reasonable steps to keep information secret.

REFERENCES

- Act of 26 June 1974 – Labour Code (consolidated text, Journal of Laws 2023 item 1465).
- Act of 16 April 1993 on Combating Unfair Competition (consolidated text, Journal of Laws 2022, item 1233).
- Będkowski-Kozioł, M. (2014). Commentary to art. 4 point 17. In T. Skoczny (Ed.). *Ustawa o ochronie konkurencji i konsumentów. Komentarz*. C. H. Beck.
- Domeij, B. (2020). The Trade Secret Directive and employees. In T. Minssen, T. Riis & J. Schovsbo (Eds.), *The harmonization and protection of trade secrets in the EU* (pp. 149–170). Edward Elgar.
- du Vall, M. & Nowińska, E. (2013). *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*. LexisNexis.
- European Convention on Human Rights. (1950, 4 November). Available at https://www.echr.coe.int/documents/d/echr/convention_ENG. Accessed 30 September 2023.
- European Commission (2012). Public consultation on the protection against misappropriation of trade secrets and confidential business information. Summary of responses, 11 December 2012, available at https://ec.europa.eu/growth/content/public-consultation-protection-against-misappropriationtrade-secrets-and-confidential_en. Accessed 30 September 2023.
- Irgens-Jensen, H. (2023). Departing employees, confidentiality clauses and European trade secret protection. *IIC – International Review of Intellectual Property and Competition Law*, 54 (pp. 495–526).
- Judgment of the Court of Appeal in Kraków of 6 December 2013, no. I ACa 1196/13.
- Judgment of the European Court of Human Rights of 12 December 2006 on the case of *Wojtunik v. Poland*, no. 64212/01.
- Judgment of the Polish Supreme Court of 3 April 2019, no. II PK 334/17.
- Judgment of the Polish Supreme Administrative Court of 9 May 2023, no. III OSK 2257/21.
- Kolasa, M. (2018). *Trade secrets and employee mobility*. Cambridge University Press.
- Korus, K. (2002). Commentary to art. 11. In K. Korus (Ed.), *Zwalczanie nieuczciwej konkurencji. Komentarz do zmian wprowadzonych ustawą z dnia 5 lipca 2002 r. o zmianie ustawy o zwalczaniu nieuczciwej konkurencji*. LEX/el.
- Korycińska-Rządca, P. (2020). *Ochrona tajemnic strony postępowania antymonopolowego w sprawach praktyk ograniczających konkurencję*. C. H. Beck.
- Michalak, A. (2006). *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*. Zakamycze.
- Michalak, A. (2016). Commentary to art. 11. In M. Sieradzka & M. Zdyb (Eds.), *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz* (pp. 386–446). Wolters Kluwer Polska.
- Nowińska, E. (2018). Commentary to art. 11. In E. Nowińska & K. Szczepanowska-Kozłowska (Eds.), *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*.
- Nowińska, E. (2022). Commentary to art. 11. In E. Nowińska & K. Szczepanowska-Kozłowska (Eds.), *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz* (pp. 234–281).
- Sołtysiński, S. & Gogulski, S. (2019). Commentary to art. 11. In J. Szwaja (Ed.). *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*. C. H. Beck.

- Traple, E. (2003). Ochrona informacji stanowiących tajemnicę przedsiębiorstwa w ZNKU a ochrona tajemnic niejawnych w trakcie negocjacji. *Monitor Prawniczy*, 21.
- Wiśniewski, A. (2023). The protection of entrepreneurs and the European Convention on Human Rights. *Białostockie Studia Prawnicze*, 28(4) (pp. 11–33). DOI: 10.15290/bsp.2023.28.04.01
- Wojcieszko-Głuszko, E. (2002). Ochrona prawna know-how w prawie polskim na tle prawnoporównawczym. *Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z wynalazczości i ochrony własności intelektualnej*, 81 (pp. 1–195).