WHISTLEBLOWING IN SERBIA AND EU DIRECTIVE

WHISTLEBLOWING IN SERBIA AND EU DIRECTIVE

Belgrade, 2023

WHISTLEBLOWING IN SERBIA AND EU DIRECTIVE

2023

Publisher
Transparency Serbia
Palmotićeva 31
Belgrade
www.transparentnost.org.rs
© 2023 Transparency Serbia

Author
Nemanja Nenadić
Transparency Serbia

Editor
Bojana Medenica
Transparency Serbia

Translation
Theotranslate

Design and layout
Marko Zakovski

Print
Unagraf, Belgrade

Copies: 100 pcs

ISBN-978-86-84711-56-6

This publication has been produced with the assistance of the Ministry of Foreign Affairs of Germany. The contents of this publication are the sole responsibility of Transparency Serbia and can in no way be taken to reflect the views of the Ministry of Foreign Affairs of Germany.

CONTENTS

FOREWORD 5

ANALYSIS OF THE DIRECTIVE FROM THE POINT OF VIEW OF POSSIBLE IMPROVEMENT OF THE LAW ON THE PROTECTION OF WHISTLEBLOWERS 7

Scope, Definitions and Conditions For Protection **7**
Internal Reporting and Follow-Up **15**
External Reporting and Follow-Up **18**
Public Disclosures **22**
Provisions Applicable to Internal and External Reporting **23**
Protection Measures **26**
Final Provisions **31**

CERTAIN WEAKNESSES OF THE LAW ON THE PROTECTION OF THE WHISTLEBLOWER 33

Definitions **33**
- Title and subject 33
- The concept of whistleblowing 33
- Whistleblower 34
- Employer, responsible person, and work engagement 35
- Competent authority for external whistleblowing 36
- Damaging action 36

Postulates **37**
- Prevention of whistleblowing and performing damaging action 37
- The conditions for the protection of whistleblowers and the issue of conscientiousness 38

Protection of persons who are not whistleblowers **41**
- Associated Persons 41
- Non-whistleblower 41
- Performing Official Duty 42
- Information seekers 43
- Unprotected reluctant whistleblowers 44

Personal data and their abuse **45**
- Protection of Whistleblower’s Personal Data 45
- Abuse of Whistleblowing 46

The process of whistleblowing **48**
- Classification 48
- Mandatory Elements 49
- Internal Whistleblowing 51
- Public Whistleblowing 57
- The data classified as secret 57

How to protect whistleblowers? **60**
- Putting whistleblowers “at a disadvantage” 60
- Compensation for Damage 61
- The rules of procedure 61
- Trainings 62
- Lawsuit 62
- Whistleblowers in labour dispute 63
- Resolving dispute through mediation 63
- Burden of proving 64
- Principle of Investigation 64
- Ruling in the absence of defendant 65
- Interim Relief 65

Monitoring the Implementation of the Law **67**
Possible penalties **67**
The beginning of law implementation **69**

“MONITORING THE IMPLEMENTATION” OF THE LAW ON PROTECTION OF WHISTLEBLOWERS 70

DID THE PROTECTION OF THE WHISTLEBLOWERS ADVANCE REPORTING OF CORRUPTION? 71

Foreword

Transparency Serbia has made proposals and comments on several occasions, first for the issuance, and then for the improvement of the Law on the Protection of Whistleblowers and its implementation. Among other things, recommendations for the improvement of this Law were published in the Business Integrity Country Agenda for Serbia (BICA).[1] We published a detailed analysis of the Law on the Protection of Whistleblowers in 2017.[2] As part of this analysis we also presented the main proposals, through which we tried to influence the improvement of several drafts of this law, as well as the proposal that was adopted in 2014. As part of Transparency Serbia, since 2005, as a regional project of Transparency International, the Anti-Corruption Legal Advisory Center has been active,[3] where we often come into contact with potential whistleblowers. This publication was produced as part of that project.

On the international scene, the Serbian Law on the Protection of Whistleblowers often received praise, which was well-deserved in terms of many provisions. There was much less talk about the shortcomings, until some of them showed up in practice. They are also referred to in the reports of the European Commission for Serbia, starting in 2019.[4] And in the latest published report (for 2022), it is stated that "the legal framework for the protection of whistleblowers has yet to be aligned with the new EU acquis".[5] Namely, it is Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. Furthermore, the reports of the European Commission present the statistics of the application of the Law (in relation to judicial protection), but also specific problems in the application of regulations: "Whistleblower reports, like in the Krušik case, have not yet been investigated in accordance with the law." Serbia must strengthen whistleblower protection and investigate allegations of high-level corruption in order to strengthen trust in institutions."[6]

Amendments to the Law on the Protection of Whistleblowers are still not part of any planning document of the Republic of Serbia, even in the context of European integration. A national strategy for the fight against corruption has not existed since 2018, and the writing of a new one by the end of 2022 had not yet begun despite numerous announcements. The action plan for Chapter 23 Negotiations with the EU also does not envisage changes in regulations, but only monitoring the situation and conducting campaigns.

Although the Law on Protection of Whistleblowers in many of its parts prescribes higher standards than the Directive does, the said harmonization could be useful, especially in terms of the actions of authorities responsible for external whistleblowing and monitoring the follow-up actions on what the whistleblowers reported. The Directive expressly stipulates that its application will in no case constitute a basis for reducing the level of protection already provided by the member states, and thus not even for Serbia, if it is harmonized. However, this work should be approached with extreme caution, because there is an inherent danger that once the procedure for amending the Law is initiated, the decision-makers, will remove from the Law some provisions that are positive under the guise of "harmonization".

The experience of the EU countries whose deadline for adopting and harmonizing regulations has already expired, would be particularly useful for making changes to the Law. However, this is delayed.[7]

Among other things, improvements are possible based on the provisions of the Directive governing:

- who is considered a person connected to the whistleblower;
- introduction of the possibility for whistleblowing channels to be managed by a third party;
- introduction of the possibility for several authorities to organize joint channels for alerting;

---

1 https://www.transparentnost.org.rs/images/dokumenti_uz_vesti/BICA_SRB_ONLINE.pdf

2 https://www.transparentnost.org.rs/images/stories/inicijativeianalize/Zakon%20o%20zastiti%20uzbunjivaca%20-%20koje%20znacenje%20normi%20igde%20se%20mogu%20poboljsati.pdf

3 https://www.transparentnost.org.rs/index.php/sr/aktivnosti-3/tekui-projekti/alac

4 https://www.mei.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/20190529-serbia-report_SR_-_REVIDIRANO.pdf

5 https://www.mei.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/Serbia_Report_2022_SR.%5B1%5D.pdf

6 https://www.mei.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/Serbia_Report_2022_SR.%5B1%5D.pdf

7 https://www.whistleblowingmonitor.eu/

- prescribing a time period for confirming the receipt of information and for providing feedback;
- prescribing conditions to be met by internal and external reporting channels;
- organizing an oral alarm (by telephone or other voice messaging system);
- designation of competent persons and services within competent authorities for external whistleblowing (currently regulated only for internal whistleblowing);
- publication of information on the method of external whistleblowing on the websites of competent authorities;
- arrangement of priorities for dealing with external alarms;
- periodic review of the effectiveness of whistleblowing channels;
- introduction of the obligation to keep records of received applications and actions of authorities;
- preventing retaliation against legal entities associated with the whistleblower;
- providing assistance to whistleblowers (counseling, cross-border cooperation);
- introduction of a general rule on no liability of whistleblowers for violations of other regulations (with necessary exceptions);
- reviewing existing offenses to determine whether sanctions are effective, proportionate and dissuasive;
- introduction of a system for creating centralized reports on whistle-blowing statistics, the implemented procedures and the amount of damage caused and compensated.

In the continuation of the publication, a detailed analysis of the Directive and possible benefits or incentives for Serbia is presented.

Analysis of the Directive from the point of view of possible improvement of the Law on the Protection of Whistleblowers

This part of the publication presents the content of *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law,*[1] compares its provisions with the rules from the Law on the Protection of Whistleblowers of the Republic of Serbia[2] (LPW) and indicates the provisions of the Directive that could be useful when considering possible improvements to that Law.

The translation of the Directive into Serbian is not official. For the purposes of this publication, the English original and the Croatian translation were used.[3]

CHAPTER I
SCOPE, DEFINITIONS AND CONDITIONS FOR PROTECTION

Article 1

Purpose

The purpose of this Directive is to enhance the enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law.

Comment:

Already from the first article, it is clear that the purpose of this Directive is to improve existing rights and regulations, through the establishment of **common minimum standards**. Therefore, in no case should compliance with the Directive be used to reduce the existing rights of whistleblowers, reduce the number of persons who are protected or reduce the obligations of state authorities and "employers" within the meaning of Law on the Protection of Whistleblowers. The inadmissibility of reducing whistleblower rights is also emphasized in one of the final provisions of the Directive.

As a downside of the Directive, when it comes to this article, it can be pointed out that its application is linked to certain predetermined areas. Regardless of how broad the field of application may be, enumerating the areas concerned by potential whistleblowing results in the emergence of situations where protection will not be provided even though it was essential to do so.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937

2 "Official Gazette of RS", number 128 of 26 November 2014.

3 https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32019L1937

Article 2

The substantive implementation of the Directive

1. This Directive lays down common minimum standards for the protection of persons reporting the following breaches of Union law:

   (a) breaches falling within the scope of the Union acts set out in the Annex that concern the following areas:

   i. public procurement;

   ii. financial services, products and markets, and prevention of money laundering and terrorist financing;

   iii. product safety and compliance;

   iv. transport safety;

   v. protection of the environment;

   vi. radiation protection and nuclear safety;

   vii. food and feed safety, animal health and welfare;

   viii. public health;

   ix. consumer protection;

   x. protection of privacy and personal data, and security of network and information systems;

   (b) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures;

   (c) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

2. This Directive is without prejudice to the power of Member States to extend protection under national law as regards areas or acts not covered by paragraph 1.

Comment:

The Directive takes the approach of pre-listing the areas to which whistleblowing may apply. LPW takes a broader approach, by defining the subject of whistleblowing as "disclosure of information on breaches of regulations, breaches of human rights, the acts of a public authority which are contrary to its entrusted purpose, the danger to life, public health, security, environment, as well as preventing large-scale damage".

The approach in the Directive is such that whistleblowing is always linked to a "breach of Union law" (that is, a breach of regulations), and then it is determined to which areas those breaches of regulations apply. On the other hand, in LPW, the subject of whistleblowing can be a breach of any regulation, and in addition, a situation when no regulation has been breached, but there is some other possible breach of public interest or some danger. Therefore, already at first glance, it can be concluded that with regard to this provision, no amendments to the LPW are necessary.

The analysis of the areas covered by the substantive implementation of the Directive leads to the same conclusion. Namely, the Republic of Serbia has regulated all the said areas with its laws. Furthermore, those regulations are largely harmonized with EU regulations. However, until full alignment with EU rules, there is a possibility that the Directive protects whistleblowers in some situations that are not covered in Serbia. However, it is not necessary to make adjustments by amending the LPW, but by amending sectoral regulations.

Article 3

Relationship with other Union acts and national provisions

1. Where specific rules on the reporting of breaches are provided for in the sector-specific Union acts listed in Part II of the Annex, those rules shall apply. The provisions of this Directive shall be applicable to the extent that a matter is not mandatorily regulated in those sector-specific Union acts.
2. This Directive shall not affect the responsibility of Member States to ensure national security or their power to protect their essential security interests. In particular, it shall not apply to reports of breaches of the procurement rules involving defence or security aspects unless they are covered by the relevant acts of the Union.
3. This Directive shall not affect the application of Union or national law relating to any of the following:
   (a) the protection of classified information;
   (b) the protection of legal and medical professional privilege;
   (c) the secrecy of judicial deliberations;
   (d) rules on criminal procedure.
4. This Directive shall not affect national rules on the exercise by workers of their rights to consult their representatives or trade unions, and on protection against any unjustified detrimental measure prompted by such consultations as well as on the autonomy of the social partners and their right to enter into collective agreements. This is without prejudice to the level of protection granted by this Directive.

Comment:

This article regulates the issue of the application of the Directive in relation to individual sectoral acts of the EU and gives primacy to the application of those rules, and only to the subsidiary application of the Directive. It is important to emphasize that the Directive will still apply if some of the sectoral regulations do not foresee obligations in the event of a breach, but, for example, only contain a recommendation for a certain way of acting.

There are as many as 11 regulations in the field of financial services, products and markets, as well as the prevention of money laundering. Among other things, those regulations govern joint investments and securities, supervision of pension insurance institutions, auditing of financial statements, market misconduct, work and supervision of the work of credit institutions, financial instruments market, etc. Also, the Annex contains Union regulations governing traffic safety (civil aviation, maritime). Finally, the annex also contains a regulation in the field of environmental protection (safety of offshore oil and gas operations).

Undoubtedly, a major shortcoming of the Directive is giving priority to the law of the member states when it comes to what those states declare to be a matter of their national security and “key security interests”. When it comes to public procurement in the field of defense and security, which is specifically mentioned, it would seem that the Directive discourages whistleblowing, leaving a wide scope for Member States to limit the rights of reporting persons. However, since EU members must apply common public procurement rules, and these rules do not allow all procurement in the security sector to be declared secret, whistleblowing of misconduct in this area will often enjoy protection.

A series of exceptions from paragraph 3 can also lead to unequal application of the Directive in various countries, depending on what their rules are when it comes to the protection of secret data, criminal proceedings, protection of professional secrecy and secrecy of court decisions.

A comparison of the presented norms shows the superiority of the current LPW in relation to what the Directive provides, but in some situations this superiority is merely apparent. LPW does not foresee the primacy of application of rules from other laws when reporting illegal actions. However, the LPW does not contain a provision that exempts the whistleblower from liability when he violates another regulation. As a result, it could happen that whistleblowers in Serbia in some cases enjoy protection that is weaker than that provided by the Directive. That would not be a good reason to harmonize the LPW with Article 3 of the Directive, but to consider its improvement, which will be discussed in connection with other provisions.

Article 4

Personal scope

1. This Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following:

   (a) persons having the status of worker, within the meaning of Article 45(1) TFEU, including civil servants;

   (b) persons having self-employed status, within the meaning of Article 49 TFEU;

   (c) shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees;

   (d) any persons working under the supervision and direction of contractors, subcontractors and suppliers.

2. This Directive shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended.

3. This Directive shall also apply to reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

4. The measures for the protection of reporting persons set out in Chapter VI shall also apply, where relevant, to:

   (a) facilitators;

   (b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and

   (c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Comment:

The personal scope of the Directive and LPW is similar, but it is somewhat wider in LPW. In Article 2, LPW stipulates, among other things, that a "whistleblower" is a natural person who blows the whistle in connection with their employment, the recruiting process, the use of the services of state and other authorities, holders of public authority or public services, business cooperation and the right of ownership of a company, while "work engagement" is full-time employment, work outside employment, volunteering, exercising a public office or any other actual work for an employer. The main advantage of the LPW, that is, the area where that Law provides a wider scope of protection than the Directive, is that whistleblowing by users of public services is protected. The main drawback of both the Directive and the LPW is that whistleblower protection is tied to the place of acquiring the information in question, or some form of connection with the institution where the breach occurred, instead of being provided to anyone who, acting in good faith, reports such a breach.

The approach to determining the connection between the whistleblower and the "employer" in these two acts is different and this may give a different outcome of application, which in some situations is more favorable for whistleblowers in Serbia. The Directive sets as a condition that the reporting person has acquired information about breaches (e.g., breach of a regulation) "in a work-related context". According to the LPW, it is not important where the whistleblower acquired the information, but whether it relates to something related to their employment, recruiting process, etc. Thus, on the basis of the Directive, the reporting of breaches of regulations that the employee learned about at work, but which has nothing to do with his work duties, would be protected, while in LPW this would be disputed. On the other hand, the LPW would give protection to reporting misconduct that is related to the work the employee performs, even in the case when they acquire this information outside of work.

The Directive is more detailed when it talks about various forms of connection of the reporting person with legal entities, but the effects are similar to those in the LPW. An interesting exception to that conclusion is the protection of persons who have acquired information as "self-employed", a term that in the context of Serbia best corresponds to the term entrepreneur. Although not mentioned in the LPW, entrepreneurs can enjoy protection in some situations, especially when they point to a breach of the law they encountered during business cooperation with a company or state authority.

The Directive and the LPW use different wording, but in both cases whistleblowing by former employees and job candidates is protected. The Directive better (less ambiguously) protects whistleblowers who have conducted unsuccessful negotiations during which they learned about a breach of the law. Protection under LPW in such situations is not certain, and depends on the broad interpretation of the term "business cooperation".

Article 4, paragraph 4 of the Directive, and especially item c), represent a norm that would improve LPW. LPW, similarly to the Directive, provides for the protection of associated persons, but this term is not defined in detail. The absence of a definition allows the concept of connected person to be interpreted broadly, but does not provide enough guarantees that it will be so in all situations. Associated persons, according to the Directive, can be those who assist the whistleblower, for example, to acquire or distribute information. Also, such facilitators may include his relatives, colleagues, friends and the like.

It is particularly significant that the Directive explicitly talks about the protection of certain legal entities, which are connected to the whistleblower. LPW does not exclude their protection, but it does not regulate it either. The protection of legal entities owned by whistleblowers or connected to them in some way is of great importance due to the extent of damage that can occur as a retaliation against business entities. This requires the need for special mechanisms, but they are not sufficiently developed even in the Directive.

Article 5

Definitions

For the purposes of this Directive, the following definitions apply:

1. 'breaches' means acts or omissions that:
   (a) are unlawful and relate to the Union acts and areas falling within the material scope referred to in Article 2; or
   (b) defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope referred to in Article 2;
2. 'information on breaches' means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches;
3. 'report' or 'to report' means, the oral or written communication of information on breaches;
4. 'internal reporting' means the oral or written communication of information on breaches within a legal entity in the private or public sector;
5. 'external reporting' means the oral or written communication of information on breaches to the competent authorities;
6. 'public disclosure' or 'to publicly disclose' means the making of information on breaches available in the public domain;
7. 'reporting person' means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities;
8. 'facilitator' means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential;

9. ‘work-related context’ means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;

10. ‘person concerned’ means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;

11. ‘retaliation’ means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;

12. ‘follow-up’ means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure;

13. ‘feedback’ means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up;

14. ‘competent authority’ means any national authority designated to receive reports in accordance with Chapter III and give feedback to the reporting person, and/or designated to carry out the duties provided for in this Directive, in particular as regards follow-up.

Comment:

Definitions of terms are among the most significant provisions in both the LPW and the Directive. As already described, the object of whistleblowing recognized by the LPW is wider, which can be seen on the example of the definition of the term “breach”[4] and “information on breaches” in the Directive. Nevertheless, the norm of the Directive is relatively broad, as it includes not only direct breaches of regulations, but also actions that are contrary to the purpose of those rules.

The term “information about a breach” is used in a similar sense as the term “information” in the LPW (Article 5, item 2), but the definition in the Directive is somewhat more clearly defined. However, the Directive also mixed various elements within the definition - what the information refers to and whether the information is correct (whether there really has been a breach), which is not good. Both acts also provide protection in cases where there has been no actual breach, but the whistleblower had reason to believe that what they reported is true. In the Directive, this degree of conviction of the whistleblower in the accuracy of the information is called “reasonable grounds”. LPW tries to objectify this belief, so it is said that the right to protection exists “if, at the time of reporting, based on the available data, a person with average knowledge and experience, as well as the whistleblower, would believe in the accuracy of the information.” Both are subject to interpretation. At this point, due to the possible consideration of the implementation of the Directive in Serbian legislation, it should be emphasized that in the Croatian text the term “reasonable grounds” is translated as “justified suspicion”, which can be detrimental to whistleblowers.

The Directive indicates more clearly than the LPW that protection is enjoyed not only for reporting a breach that occurred (or one the whistleblower believed has occurred), but also in those situations where there is a “highly probable” risk that the rule will be breached. The Serbian LPW does not contain such a rule and the Directive could be used as a reason for its improvement. Also, the Directive indicates somewhat more clearly than the LPW that whistleblowing can also include an attempt to conceal the fact that a breach has occurred. At this point, one more advantage of the Directive can be mentioned - the LPW binds the right to protection for certain timeframes in relation to the time when the breach referred to occurred, while the Directive does not. In other words, based on the Directive, the reporting person can receive protection regardless of when the misconduct occurred and when they found out about it, while in LPW there are both objective and subjective periods (10 and 1 year, respectively).

4 In this text, the term “breach” is used, taken from the Croatian translation. LPW does not contain a single term that would cover everything that can be the subject of whistleblowing.

Although the term "whistleblower" and "whistleblowing" have become common in the Serbian language, in the translation of the Directive in this analysis, the terms "report" and "reporting person" were used, akin to the original English text, as well as in the Croatian translation. It is particularly useful for understanding the difference between the two acts. Furthermore, "reporting person" is a value-neutral term, and it is quite appropriate to include both the persons who will receive protection under the Directive and those who do not qualify for it. On the other hand, "whistleblower" has a positive connotation, but based on the LPW, it includes both persons who blow the whistle in accordance with the rules and those who breach them.

Both acts recognize internal and external whistleblowing, as well as informing the public.

In both acts, the whistleblower can only be a natural person.

The definition of "work-related context" in the Directive indicates that it is in this context that the reporting person may experience retaliation. The LPW also covers situations when the detrimental action against the whistleblower is carried out elsewhere or by someone else, not only the employer, which is better. However, the protection rules in such cases are not sufficiently developed.

The Directive, unlike the LPW, contains a definition of "person concerned" and deals with the protection of their rights to a much greater extent than the LPW, which is useful.

The definition of "retaliation" in the Directive and "detrimental action" in the LPW are similar, although there is also a difference, the scope of which could only be assessed based on a detailed analysis of jurisprudence. In Serbian law, detrimental action is considered to include actions that are "in connection with whistleblowing", and in the Directive, such action should be "prompted by" reporting. The LPW provides for protection in case of endangering or violating the whistleblower's rights or putting them in a disadvantageous position, while the Directive talks about "unjustified detriment". Here too, only practice can show which definition is more complete, but it seems that the definition of LPW should not be changed, but perhaps only supplemented with elements from the Directive.

The Directive pays more attention to the action taken after the whistleblowing, so the definitions already define what "follow-up" and "feedback" are.

Article 6

Conditions for protection of reporting persons

1. Reporting persons shall qualify for protection under this Directive provided that:

   (a) they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this Directive; and

   (b) they reported either internally in accordance with Article 7 or externally in accordance with Article 10, or made a public disclosure in accordance with Article 15.

2. Without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, this Directive does not affect the power of Member States to decide whether legal entities in the private or public sector and competent authorities are required to accept and follow up on anonymous reports of breaches.

3. Persons who reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection provided for under Chapter VI, provided that they meet the conditions laid down in paragraph 1.

4. Persons reporting to relevant institutions, bodies, offices or agencies of the Union breaches falling within the scope of this Directive shall qualify for protection as laid down in this Directive under the same conditions as persons who report externally.

Comment:

Conceptually, the Directive and LPW set conditions similarly for the protection of whistleblowers. As already explained, protection is also provided in the case when the whistleblower had reason to believe in the truth and relevance of what they report and when they have followed the prescribed reporting procedure. LPW sets timeframes that are not provided for in the Directive.

The Directive opens the possibility, but does not create an obligation, for member states to allow and protect anonymous reporting. In LPW, the duty to act on anonymous notifications has been established. Both acts also protect a person who suffers retaliation for reporting anonymously, if their identity is subsequently revealed.

CHAPTER II

INTERNAL REPORTING AND FOLLOW-UP

Article 7

Reporting through internal reporting channels

1. As a general principle and without prejudice to Articles 10 and 15, information on breaches may be reported through the internal reporting channels and procedures provided for in this Chapter.

2. Member States shall encourage reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation.

3. Appropriate information relating to the use of internal reporting channels referred to in paragraph 2 shall be provided in the context of the information given by legal entities in the private and public sector pursuant to point (g) of Article 9(1), and by competent authorities pursuant to point (a) of Article 12(4) and Article 13.

Comment:

Whistleblowing is recognized in both acts. The Directive is not entirely clear when it comes to "encouraging the prioritization" of internal whistleblowing over other forms of whistleblowing. There is no such rule in the LPW, but the whistleblower, in principle, can choose which channel to use, except in some special cases (e.g., dealing with secret data).

Article 8

Obligation to establish internal reporting channels

1. Member States shall ensure that legal entities in the private and public sector establish channels and procedures for internal reporting and for follow-up, following consultation and in agreement with the social partners where provided for by national law.

2. The channels and procedures referred to in paragraph 1 of this Article shall enable the entity's workers to report information on breaches. They may enable other persons, referred to in points (b), (c) and (d) of Article 4(1) and Article 4(2), who are in contact with the entity in the context of their work-related activities to also report information on breaches.

3. Paragraph 1 shall apply to legal entities in the private sector with 50 or more workers.

4. The threshold laid down in paragraph 3 shall not apply to the entities falling within the scope of Union acts referred to in Parts I.B and II of the Annex.

5. Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party. The safeguards and requirements referred to in Article 9(1) shall also apply to entrusted third parties operating the reporting channel for a legal entity in the private sector.

6. Legal entities in the private sector with 50 to 249 workers may share resources as regards the receipt of reports and any investigation to be carried out. This shall be without prejudice to the obligations imposed upon such entities by this Directive to maintain confidentiality, to give feedback, and to address the reported breach.

7. Following an appropriate risk assessment taking into account the nature of the activities of the entities and the ensuing level of risk for, in particular, the environment and public health, Member States may require legal entities in the private sector with fewer than 50 workers to establish internal reporting channels and procedures in accordance with Chapter II.

8. Member States shall notify the Commission of any decision they take to require legal entities in the private sector to establish internal reporting channels pursuant to paragraph 7. That notification shall include the reasons for the decision and the criteria used in the risk assessment referred to in paragraph 7. The Commission shall communicate that decision to the other Member States.

9. Paragraph 1 shall apply to all legal entities in the public sector, including any entity owned or controlled by such entities.

   Member States may exempt from the obligation referred to in paragraph 1 municipalities with fewer than 10,000 inhabitants or fewer than 50 workers, or other entities referred to in the first subparagraph of this paragraph with fewer than 50 workers.

   Member States may provide that internal reporting channels can be shared between municipalities or operated by joint municipal authorities in accordance with national law, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels.

Comment:

The concept of internal whistleblowing is similar in both acts. The provisions of LPW are generally more demanding than those contained in the Directive, especially when it comes to the private sector. Among other things, every employer with more than 10 employees must pass an act regulating the internal whistleblowing procedure, while according to the Directive, the obligation to establish such a system exists when there are more than 50 employees.

However, in this article of the Directive there are also some provisions that would be useful to have in the LPW. One of them is giving the opportunity to report internally not only to employees within the legal entity, but also to external collaborators of the institution (Article 8, paragraph 5). Providing such an opportunity in LPW would relieve numerous employers from the public and private sector, and as a result, there could be a more professional and impartial handling of reports.

Similarly (Article 8, paragraph 6) foresees a useful possibility that LPW does not provide for - that several legal entities may share resources as regards the receipt of reports and any investigation. In the Directive, such an opportunity is provided to companies with less than 250 employees.

When it comes to the public sector, the Directive is more demanding than the LPW - it is set as a rule that every public sector entity must establish an internal reporting channel. However, there is room for significant exceptions (bodies with less than 50 employees), while in LPW the limit is set lower (10).

Similar to the private sector, the Directive indicates the possibility for some entities in the public sector (municipalities) to establish a common internal whistleblowing system. This useful possibility does not exist in LPW.

Article 9

The procedures for internal reporting and for follow-up

1. The procedures for internal reporting and for follow-up as referred to in Article 8 shall include the following:

   (a) channels for receiving the reports which are designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report is protected, and prevents access thereto by non-authorised staff members;

   (b) acknowledgment of receipt of the report to the reporting person within seven days of that receipt;

   (c) the designation of an impartial person or department competent for following-up on the reports which may be the same person or department as the one that receives the reports and which will maintain communication with the reporting person and, where necessary, ask for further information from and provide feedback to that reporting person;

   (d) diligent follow-up by the designated person or department referred to in point (c);

   (d) diligent follow-up, where provided for in national law, as regards anonymous reporting;

   (f) a reasonable timeframe to provide feedback, not exceeding three months from the acknowledgment of receipt or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made;

   (g) provision of clear and easily accessible information regarding the procedures for reporting externally to competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union.

2. The channels provided for in point (a) of paragraph 1 shall enable reporting in writing or orally, or both. Oral reporting shall be possible by telephone or through other voice messaging systems, and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

Comment:

Article 9 of the Directive regulates the internal reporting channels in more detail than the LPW does, so it would be possible to improve the Serbian Law based on the Directive. Some of the issues addressed by the Directive have been resolved in Serbia by the Rulebook of the Ministry of Justice and internal acts, which are mostly drawn up according to the same model.

The Directive could be used to improve the rules on the security of the reporting channel, to ensure the protection of confidentiality and to introduce certain timeframes that are not currently prescribed.

In Serbia, there is a prescribed period in which authorities and companies must act on the received information, and that is 15 days. Also, there is a duty to inform the whistleblower about the outcome of the initiated procedure, 15 days after the procedure has ended. On the other hand, the Directive recognizes a "reasonable timeframe for providing feedback", which cannot exceed three months. The Directive is not clear enough here - whether procedures must be completed within three months or just initiated based on the report. If it were to be interpreted that there is a duty to complete the proceedings within a certain timeframe, the Directive could be used to improve the LPW, which currently does not contain such a timeframe.

Another useful rule in the Directive is the obligation of the services in charge of internal reporting to provide interested parties with information about who could be responsible for external reporting.

The Directive gives more options than the LPW when it comes to oral reporting. While in Serbia it is possible to report "orally for the record", the Directive also refers to reporting by phone or other voice message system. This possibility should also be prescribed in the LPW.

CHAPTER III
EXTERNAL REPORTING AND FOLLOW-UP

Article 10

Reporting through external reporting channels

Without prejudice to point (b) of Article 15(1), reporting persons shall report information on breaches using the channels and procedures referred to in Articles 11 and 12, after having first reported through internal reporting channels, or by directly reporting through external reporting channels.

Article 11

Obligation to establish external reporting channels and to follow up on reports

1. Member States shall designate the authorities competent to receive, give feedback and follow up on reports, and shall provide them with adequate resources.

2. Member States shall ensure that the competent authorities:

   (a) establish independent and autonomous external reporting channels, for receiving and handling information on breaches;

   (b) promptly, and in any event within seven days of receipt of the report, acknowledge that receipt unless the reporting person explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of the report would jeopardise the protection of the reporting person's identity;

   (c) diligently follow up on the reports;

   (d) provide feedback to the reporting person within a reasonable timeframe not exceeding three months, or six months in duly justified cases;

   (e) communicate to the reporting person the final outcome of investigations triggered by the report, in accordance with procedures provided for under national law;

   (f) transmit in due time the information contained in the report to competent institutions, bodies, offices or agencies of the Union, as appropriate, for further investigation, where provided for under Union or national law.

3. Member States may provide that competent authorities, after having duly assessed the matter, can decide that a reported breach is clearly minor and does not require further follow-up pursuant to this Directive, other than closure of the procedure. This shall not affect other obligations or other applicable procedures to address the reported breach, or the protection granted by this Directive in relation to internal or external reporting. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

4. Member States may provide that competent authorities can decide to close procedures regarding repetitive reports which do not contain any meaningful new information on breaches compared to a past report in respect of which the relevant procedures were concluded, unless new legal or factual circumstances justify a different follow-up. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

5. Member States may provide that, in the event of high inflows of reports, competent authorities may deal with reports of serious breaches or breaches of essential provisions falling within the scope of this Directive as a matter of priority, without prejudice to the timeframe as set out in point (d) of paragraph 2.

6. Member States shall ensure that any authority which has received a report but does not have the competence to address the breach reported transmits it to the competent authority, within a reasonable time, in a secure manner, and that the reporting person is informed, without delay, of such a transmission.

Comment:

In the case of external whistleblowing, it is good that the Directive obliges member states to provide appropriate means for the work of competent authorities. There is no such norm in LPW, which is not so much a problem as the fact that many state authorities are not aware that they are responsible for external whistleblowing and that they should seek funds to perform this function.

Similar to the case of internal reporting, here too, the Directive, depending on the interpretation, could serve as an occasion to specify the timeframes in the domestic law. The LPW stipulates a timeframe of 15 days for informing the whistleblower from receiving of the report and 15 days from the end of the procedure initiated upon the report, but the duration of that procedure is not subject to a timeframe. On the other hand, the Directive mandates to provide feedback within three months, which can be extended to six months. Furthermore, the Directive sets the obligation to inform the reporting person about the "final outcome of the investigation", which nevertheless indicates that the procedure could last even longer than the said timeframe.

The Directive gives the possibility to suspend the procedure in case of "minor breaches", which is not explicitly mentioned by the LPW, but it can undoubtedly happen based on other regulations applied by competent authorities (e.g., inspections). Even when the reported breach is minor, both acts protect the person who made the report from retaliation. The Directive expressly mentions the possibility of not following up on a new report in the same matter when the procedure on the previous one has been closed, and there are meaningful new information LPW does not mention it, but the same outcome is reached by applying other regulations.

Unlike the LPW, the Directive indicates the possibility that the competent authority prioritize the treatment of reports according to the severity of the reported breach. Introducing such a provision would be useful in Serbian Law as well.

Article 12

Design of external reporting channels

1. External reporting channels shall be considered independent and autonomous, if they meet all of the following criteria:

   (a) they are designed, established and operated in a manner that ensures the completeness, integrity and confidentiality of the information and prevents access thereto by non-authorised staff members of the competent authority;

   (b) they enable the durable storage of information in accordance with Article 18 to allow further investigations to be carried out.

2. The external reporting channels shall enable reporting in writing and orally. Oral reporting shall be possible by telephone or through other voice messaging systems and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

3. Competent authorities shall ensure that, where a report is received through channels other than the reporting channels referred to in paragraphs 1 and 2 or by staff members other than those responsible for handling reports, the staff members who receive it are prohibited from disclosing any information that might identify the reporting person or the person concerned, and that they promptly forward the report without modification to the staff members responsible for handling reports.

4. Member States shall ensure that competent authorities designate staff members responsible for handling reports, and in particular for:

   (a) providing any interested person with information on the procedures for reporting;

   (b) receiving and following up on reports;

   (c) maintaining contact with the reporting person for the purpose of providing feedback and requesting further information where necessary.

5. The staff members referred to in paragraph 4 shall receive specific training for the purposes of handling reports.

Comment:

> The Directive in Article 12 regulates in a more complete manner the external reporting channels relative to the LPW, so these provisions could be used as inspiration for improving the Serbian Law.

Article 13

Information regarding the receipt of reports and their follow-up

Member States shall ensure that competent authorities publish on their websites in a separate, easily identifiable and accessible section at least the following information:

(a) the conditions for qualifying for protection under this Directive;

(b) the contact details for the external reporting channels as provided for under Article 12, in particular the electronic and postal addresses, and the phone numbers for such channels, indicating whether the phone conversations are recorded;

(c) the procedures applicable to the reporting of breaches, including the manner in which the competent authority may request the reporting person to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of such feedback.

(d) the confidentiality regime applicable to reports, and in particular the information in relation to the processing of personal data in accordance with Article 17 of this Directive, Articles 5 and 13 of Regulation (EU) 2016/679, Article 13 of Directive (EU) 2016/680 and Article 15 of Regulation (EU) 2018/1725, as applicable;

(e) the nature of the follow-up to be given to reports;

(f) the remedies and procedures for protection against retaliation and the availability of confidential advice for persons contemplating reporting;

(g) a statement clearly explaining the conditions under which persons reporting to the competent authority are protected from incurring liability for a breach of confidentiality pursuant to Article 21(2); and

(h) contact details of the information centre or of the single independent administrative authority as provided for in Article 20(3) where applicable.

Comment:

> Article 13 of the Directive could also be a good model for the improvement of LPW. Namely, LPW does not set rules at all regarding the way of informing potentially interested persons about the possibilities they have with external whistleblowing. The Directive stipulates what information each competent authority should publish on its website. In Serbia, state authorities should publish part of this information based on their obligations from other regulations, primarily the Law on Free Access to Information of Public Importance, within the framework of information about work. However, it would be both useful and appropriate to regulate this issue in the Law on the Protection of Whistleblowers itself.

Article 14

Review of the procedures by competent authorities

Member States shall ensure that competent authorities review their procedures for receiving reports, and their follow-up, regularly, and at least once every three years. In reviewing such procedures, competent authorities shall take account of their experience as well as that of other competent authorities and adapt their procedures accordingly.

Comment:

In order to improve whistleblowing in Serbia, it would be very useful if the LPW contained an obligation from Article 14 of the Directive, that competent state authorities periodically consider whether the procedure for external whistleblowing is of sufficient quality and then taking account of their experience as well as that of other competent authorities adapt their procedures accordingly.

CHAPTER IV

PUBLIC DISCLOSURES

Article 15

Public Disclosures

1. A person who makes a public disclosure shall qualify for protection under this Directive if any of the following conditions is fulfilled:

   (a) the person first reported internally and externally, or directly externally in accordance with Chapters II and III, but no appropriate action was taken in response to the report within the timeframe referred to in point (f) of Article 9(1) or point (d) of Article 11(2); or

   (b) the person has reasonable grounds to believe that:

      i. the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or

      ii. in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

2. This Article shall not apply to cases where a person directly discloses information to the press pursuant to specific national provisions establishing a system of protection relating to freedom of expression and information.

Comment:

The norms on “whistleblowing to the public” in the LPW (Article 19 and 20) are more restrictive than the provisions on “public disclosures” from the Directive (Article 15). Thus, based on the Directive, there is a possibility for the whistleblower to address the public whenever internal or external whistleblowing has not been successful, either if the reporting persons did not receive information within the timeframe required or no appropriate action was taken following the report.

On the other hand, the LPW protects such disclosure of information only in case of immediate danger to life, public health, safety, environment, from the occurrence of large-scale damage or if there is an immediate danger of destruction of evidence. The Directive too recognizes some of these grounds, so protection will be provided to a person who has directly addressed the public, and has reasonable grounds to suspect that there could be an immediate danger to the public interest, when there is a risk of retaliation, concealment or destruction of evidence as a result of external reporting.

In the LPW (Article 18, paragraph 2), instead of the right for a whistleblower who doubts the impartiality of a competent authority to address the public directly, the possibility of addressing an immediate superior authority is foreseen (e.g. the ministry instead of the municipal inspection, the appellate instead of the higher public prosecutor’s office). In addition, the LPW does not explicitly recognize as grounds for directly addressing the public a situation in which there is suspicion of collusion between the representative of the competent authority and the person participating in the breach of regulations.

The Directive in Article 15, paragraph 2, refers to the application of regulations on the protection of freedom of expression and information, when the whistleblower addresses the media. LPW does not regulate these issues, and it would be necessary to at least consider whether there is a possible collision of norms.

CHAPTER V

PROVISIONS APPLICABLE TO INTERNAL AND EXTERNAL REPORTING

Article 16

Duty of confidentiality

1. Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced.

2. By way of derogation from paragraph 1, the identity of the reporting person and any other information referred to in paragraph 1 may be disclosed only where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned.

3. Disclosures made pursuant to the derogation provided for in paragraph 2 shall be subject to appropriate safeguards under the applicable Union and national rules. In particular, reporting persons shall be informed before their identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings. When informing the reporting persons, the competent authority shall send them an explanation in writing of the reasons for the disclosure of the confidential data concerned.

4. Member States shall ensure that competent authorities that receive information on breaches that includes trade secrets do not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up.

Comment:

The LPW and the Directive have a similar starting point when it comes to the confidentiality of whistleblower identity. The Directive pays more attention to maintaining confidentiality within the institution addressed by the whistleblower. Also, it is clearly indicated (Article 16, paragraph 1) that not only identification data should be stored, but also any other information from which the identity of the reporting person may be directly or indirectly deduced These additions could also be useful in LPW.

The Directive leaves a lot of room for disclosing the identity of the reporting person. It mentions the possibility of disclosing that information for the purposes of conducting an investigation and judicial proceedings, but also in other situations, when it is provided for by national legislation, and the obligation is "necessary and proportionate". LPW norms are even more unfavorable. In Article 18, the LPW does stipulate that a non-competent authority may not disclose the whistleblower's identity to the authority competent to act, but the rule is relativized by the fact that the identity will still be disclosed if (any) law prescribes otherwise. Similarly, in Article 10, paragraph 3, the LPW provides for the possibility of disclosing the whistleblower's identity to the competent authority, "if without disclosure the action of that authority would be impossible". These norms of LPW should be reviewed, whereby the Directive can serve as one of the arguments. First of all, the situations where there is a need to reveal the whistleblower's identity should be determined, and based on that, adequate solutions should be formulated. This was not done during the drafting of the LPW.

Particularly dangerous for whistleblowers can be the provision of the Directive, where the reason for identity disclosure is "safeguarding the rights of defense of the person concerned". On the other hand, the LPW expressly states (Article 10, paragraph 5) that the whistleblower's identity cannot be revealed to "the person referred to in the information", but at the same time relativizes this rule ("unless otherwise prescribed by a separate law").

The best protection for both the reporting person and the concerned person is a prompt and impartial investigation of the reported breach. Revealing the whistleblower's identity while this investigation is ongoing would be inappropriate and prejudicial. Only if it is established that the report was false

could there be a legitimate interest of the person concerned to know who reported them. Neither the Directive nor the LPW set this rule.

Article 16, paragraph 4, regulates the duty to keep trade secrets, when such information is provided in the report. While the LPW does not address this issue, it could be very significant.

Article 17

Processing of personal data

Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices or agencies shall be undertaken in accordance with Regulation (EU) 2018/1725.

Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

Comment:

Article 17

Similar to the Directive, the LPW refers to the application of regulations on the protection of personal data. LPW contains a rule (in Article 19, which refers to public whistleblowing) that the whistleblower is obliged to respect the right to protection of personal data. The Directive in this article regulates the actions of legal entities and state authorities, so it orders the deletion of data that are not relevant for handling a specific report, but it remains unclear whether this means that the authority would remove those irrelevant personal data from the report, if it is forwarded to someone.

Article 18

Record keeping of the reports

1. Member States shall ensure that legal entities in the private and public sector and competent authorities keep records of every report received, in compliance with the confidentiality requirements provided for in Article 16. Reports shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by this Directive, or other requirements imposed by Union or national law.

2. Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the reporting person, legal entities in the private and public sector and competent authorities shall have the right to document the oral reporting in one of the following ways:

   (a) by making a recording of the conversation in a durable and retrievable form; or

   (b) through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report.

   Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the transcript of the call by signing it.

3. Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, legal entities in the private and public sector and competent authorities shall have the right to document the oral reporting in the form of accurate minutes of the conversation written by the staff member responsible for handling the report. Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the minutes of the conversation by signing them.

4. Where a person requests a meeting with the staff members of legal entities in the private and public sector or of competent authorities for reporting purposes pursuant to Articles 9(2) and 12(2), legal entities in the private and public sector and competent authorities shall ensure, subject to the consent of the reporting person, that complete and accurate records of the meeting are kept in a durable and retrievable form

   Legal entities in the private and public sector and competent authorities shall have the right to document the meeting in one of the following ways:

   (a) by making a recording of the conversation in a durable and retrievable form; or

   (б) through accurate minutes of the meeting prepared by the staff members responsible for handling the report.

   Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the minutes of the meeting by signing them.

This article of the Directive regulates certain matters that are not regulated in the LPW, and which would be useful to address in that Law. It concerns keeping records of reports.

CHAPTER VI
PROTECTION MEASURES

Article 19

Prohibition of retaliation

Member States shall take the necessary measures to prohibit any form of retaliation against persons referred to in Article 4, including threats of retaliation and attempts of retaliation including in particular in the form of:

(a) suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a licence or permit;

(o) psychiatric or medical referrals.

Comment:

The Directive and the LPW take a similar approach when they prohibit retaliation (detrimental action) taken against whistleblowers and other protected persons. In principle, any form of retaliation is prohibited, and some of them are explicitly listed in Article 19 and Directive, i.e. Article 21 of the Law.

Although the list is not exhaustive, it can be useful to some extent, as it establishes a legal presumption that a specific conduct is illegal. The list of these detrimental actions in the two acts often overlaps and refers to cases of retaliation that mainly affect employees.

As examples from the Directive that are not mentioned by the LPW, it should be highlighted in particular the employer's failure to convert a temporary employment contract into a permanent one, where the employee had legitimate expectations that he or she would be offered permanent employment, being blacklisted, early termination or cancellation of a contract for goods or services, license or permit cancellation, harm to the person's reputation, and financial losses. As can be seen, some of these examples involve retaliation against a legal entity associated with the reporting person. As stated earlier, the Serbian Law does not exclude the possibility of considering legal entities as

persons connected to the whistleblower, but it does not elaborate on the prevention and elimination of detrimental consequences suffered by legal entities.

Another provision from the Directive that would be useful for the LPW is the introductory part of Article 19, where it is expressly prohibits retaliation, including threats of retaliation and attempts of retaliation.

Article 20

Measures of support

1 Member States shall ensure that persons referred to in Article 4 have access, as appropriate, to support measures, in particular the following:

(a) comprehensive and independent information and advice, which is easily accessible to the public and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned;

(b) effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, including, where provided for under national law, certification of the fact that they qualify for protection under this Directive; and

(c) legal aid in criminal and in cross-border civil proceedings in accordance with Directive (EU) 2016/1919 and Directive 2008/52/EC of the European Parliament and of the Council (48), and, in accordance with national law, legal aid in further proceedings and legal counselling or other legal assistance.

2. Member States may provide for financial assistance and support measures, including psychological support, for reporting persons in the framework of legal proceedings.

3. The support measures referred to in this Article may be provided, as appropriate, by an information centre or a single and clearly identified independent administrative authority.

Comment:

The Directive regulates certain useful support measures that are not mentioned or not sufficiently elaborated in the LPW. This refers to the provision of comprehensive information and advice, but even more so to the assistance of competent authorities in the protection against retaliation, both in the country and abroad. Also, the Directive indicates the possibility for member states to provide financial and psychological assistance to whistleblowers.

The Directive envisages a centralized provision of assistance to reporting persons, whether it is an administrative authority or an information center. In Serbia, a single state body has not been vested with such competences, although the Ministry of Justice published some information after the adoption of the LPW.

Particularly interesting is the option left by the Directive for reporting persons to be issued with a certification of the fact that they qualify for protection under the Directive. This is very similar to the granting of “whistleblower status” that existed in Serbia before the adoption of the LPW. Now such a possibility does not exist.

Article 21

Measures for protection against retaliation

1. Member States shall take the necessary measures to ensure that persons referred to in Article 4 are protected against retaliation. Such measures shall include, in particular, those set out in paragraphs 2 to 8 of this Article.

2. Without prejudice to Article 3(2) and (3), where persons report information on breaches or make a public disclosure in accordance with this Directive they shall not be considered to have breached any restriction on disclosure of information and shall not incur liability of any kind in respect of such a report or public disclosure provided that they had reasonable grounds to believe that the reporting or public disclosure of such information was necessary for revealing a breach pursuant to this Directive.

3. Reporting persons shall not incur liability in respect of the acquisition of or access to the information which is reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence. In the event of the acquisition or access constituting a self-standing criminal offence, criminal liability shall continue to be governed by applicable national law.

4. Any other possible liability of reporting persons arising from acts or omissions which are unrelated to the reporting or public disclosure or which are not necessary for revealing a breach pursuant to this Directive shall continue to be governed by applicable Union or national law.

5. In proceedings before a court or other authority relating to a detriment suffered by the reporting person, and subject to that person establishing that he or she reported or made a public disclosure and suffered a detriment, it shall be presumed that the detriment was made in retaliation for the report or the public disclosure. In such cases, it shall be for the person who has taken the detrimental measure to prove that that measure was based on duly justified grounds.

6. Persons referred to in Article 4 shall have access to remedial measures against retaliation as appropriate, including interim relief pending the resolution of legal proceedings, in accordance with national law.

7. In legal proceedings, including for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective labour law, persons referred to in Article 4 shall not incur liability of any kind as a result of reports or public disclosures under this Directive. Those persons shall have the right to rely on that reporting or public disclosure to seek dismissal of the case, provided that they had reasonable grounds to believe that the reporting or public disclosure was necessary for revealing a breach, pursuant to this Directive.

   Where a person reports or publicly discloses information on breaches falling within the scope of this Directive, and that information includes trade secrets, and where that person meets the conditions of this Directive, such reporting or public disclosure shall be considered lawful under the conditions of Article 3(2) of the Directive (EU) 2016/943.

8. Member States shall take the necessary measures to ensure that remedies and full compensation are provided for damage suffered by persons referred to in Article 4 in accordance with national law.

Comment:

The Directive provides a general rule on the duty of states to take measures to protect against retaliation, and then lists some of them.

The Directive contains one very important rule that is not in the LPW - that a person who has made a public disclosure of a breach, while having respected the rules contained in the Directive, but nonetheless exceeded restrictions regarding the disclosure of information, shall not incur liability of any kind in respect of such a report or public disclosure. True, this rule is very limited with many exceptions (national security, judicial secrecy, etc.) Therefore, the Directive could be used as an occasion to remedy this major deficiency of LPW and to discuss the best ways to do so.

LPW also specifically regulates whistleblowing that is done using confidential data. The special procedure in Article 20 implies addressing the "employer" and then the authorized body. The whistleblower cannot go public with secret information "if the law does not prescribe otherwise" (and it is not prescribed anywhere, or at least not in a clear way).

The Directive also regulates the issue of the reported person's liability for obtaining information. The LPW does not address this issue, so it may happen that a whistleblower suffers detrimental consequences if he obtained information unlawfully, but is protected from prosecution for sharing that information with others.

The Directive, like the LPW, introduces an important presumption that the detrimental action was taken in retaliation for reporting. This reverses the burden of proof, so the one who undertakes a detrimental action must prove that there are some justified reasons for it. LPW regulates this issue in more detail than the Directive.

The Directive mentions as one of the legal means of protection interim remedies pending the resolution of legal proceedings, which is elaborated in more detail in the LPW and other regulations.

In paragraph 7 of this Article, the Directive indicates some other cases of exemption from liability, which LPW does not mention (breach of copyright, breach of data secrecy, disclosure of trade secrets, etc.). It is expressly stated that the reporting persons meeting certain conditions, have the right to ask the court to dismiss the case against them. This is also one of the issues that deserve discussion in Serbia, with the aim of possible improvement of LPW. In this regard, it would be particularly important to establish whether the courts grant rights to whistleblowers who point out this type of detrimental actions, and at what stage of the judicial proceedings this happens (interim relief or final decision).

In terms of damages, the Directive only refers to national law and "full compensation for damage suffered". The LPW regulates this issue in some detail, but insufficiently.

Article 22

Measures for protection of persons concerned

1. Member States shall ensure, in accordance with the Charter, that persons concerned fully enjoy the right to an effective remedy and to a fair trial, as well as the presumption of innocence and the rights of defence, including the right to be heard and the right to access their file.

2. Competent authorities shall ensure, in accordance with national law, that the identity of persons concerned is protected for as long as investigations triggered by the report or the public disclosure are ongoing.

3. The rules set out in Articles 12, 17 and 18 as regards the protection of the identity of reporting persons shall also apply to the protection of the identity of persons concerned.

The rights of persons who are the subject of whistleblowing reports (e.g. possible perpetrators of criminal acts) are somewhat more elaborated in the Directive than in the LPW, which relies on other regulations in this respect. An issue that has not been sufficiently resolved in Serbia is the protection of the identity of persons concerned (e.g., within the authority to which the case was reported, in communication between authorities).

Article 23

Penalties

1. Member States shall provide for effective, proportionate and dissuasive penalties applicable to natural or legal persons that:

    (a) hinder or attempt to hinder reporting;

    (b) retaliate against persons referred to in Article 4;

    (c) bring vexatious proceedings against persons referred to in Article 4;

    (d) breach the duty of maintaining the confidentiality of the identity of reporting persons, as referred to in Article 16.

2. Member States shall provide for effective, proportionate and dissuasive penalties applicable in respect of reporting persons where it is established that they knowingly reported or publicly disclosed false information. Member States shall also provide for measures for compensating damage resulting from such reporting or public disclosures in accordance with national law.

Comment:

The Directive, as well as the LPW, provides for penalties in case of breach of the rules. The Directive does not describe the nature and amount of penalties that should be established, but it contains general rules - that they should be effective, proportionate and dissuasive. Based on that, a discussion could be opened in Serbia about the adequacy of the penalties that are currently prescribed and about their effects. Only in this way could it be determined whether they meet these three requirements from the Directive.

When it comes to actions and omissions for which penalties should be prescribed, although the number of offenses in the LPW is wider, some of the offenses from the Directive are not listed. Thus, the LPW does not prescribe a penalty for hindering a report or reporting by a whistleblower, as well as for those who breach the duty of maintaining the confidentiality of the identity of the reporting person. LPW provides for a misdemeanour penalty for an employer who fails to protect a whistleblower from a detrimental action, but not for another person who undertakes a detrimental action towards the whistleblower or initiates vexatious proceedings against him.

LPW also does not contain a misdemeanour penalty for a reporting person who has knowingly provided false information. In some cases, there is a possibility that such reporting persons may be prosecuted (false reporting, defamation).

Article 24

No waiver of rights and remedies

Member States shall ensure that the rights and remedies provided for under this Directive cannot be waived or limited by any agreement, policy, form or condition of employment, including a pre-dispute arbitration agreement.

Comment:

The Directive, as well as the LPW, prohibits agreements that would limit the rights of reporting persons/whistleblowers.

CHAPTER VII

FINAL PROVISIONS

Article 25

More favourable treatment and non-regression clause

1. Member States may introduce or retain provisions more favourable to the rights of reporting persons than those set out in this Directive, without prejudice to Article 22 and Article 23(2).

2. The implementation of this Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by this Directive.

Comment:

> If Serbia were to decide to harmonize its LPW with the Directive, this would be the most important provision to keep in mind.

Article 26

Transposition and transitional period

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 17 December 2021.

2. By way of derogation from paragraph 1, as regards legal entities in the private sector with 50 to 249 workers, Member States shall by 17 December 2023 bring into force the laws, regulations and administrative provisions necessary to comply with the obligation to establish internal reporting channels under Article 8(3).

3. When Member States adopt the provisions referred to in paragraphs 1 and 2, those provisions shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made. They shall forthwith communicate to the Commission the text of those provisions.

Comment:

> Just over a year has passed since the deadline for the implementation of the Directive in the EU member states. That period is relatively short, but it is enough to show which norms were the most problematic in practice, and which produced the best effects.

Article 27

Reporting, evaluation and review

1. Member States shall provide the Commission with all relevant information regarding the implementation and application of this Directive. On the basis of the information provided, the. Commission shall, by 17 December 2023, submit a report to the European Parliament and the Council on the implementation and application of this Directive.

2. Without prejudice to reporting obligations laid down in other Union legal acts, Member States shall, on an annual basis, submit the following statistics on the reports referred to in Chapter III to the Commission, preferably in an aggregated form, if they are available at a central level in the Member State concerned:

   (a) the number of reports received by the competent authorities;

(b) the number of investigations and proceedings initiated as a result of such reports and their outcome; and

(c) if ascertained, the estimated financial damage, and the amounts recovered following investigations and proceedings, related to the breaches reported.

3. The Commission shall, by 17 December 2025, taking into account its report submitted pursuant to paragraph 1 and the Member States' statistics submitted pursuant to paragraph 2, submit a report to the European Parliament and to the Council assessing the impact of national law transposing this Directive. The report shall evaluate the way in which this Directive has functioned and consider the need for additional measures, including, where appropriate, amendments with a view to extending the scope of this Directive to further Union acts or areas, in particular the improvement of the working environment to protect workers' health and safety and working conditions.

   In addition to the evaluation referred to in the first subparagraph, the report shall evaluate how Member States made use of existing cooperation mechanisms as part of their obligations to follow up on reports regarding breaches falling within the scope of this Directive and more generally how they cooperate in cases of breaches with a cross-border dimension.

4. The Commission shall make the reports referred to in paragraphs 1 and 3 public and easily accessible.

This is one of the most important provisions of the Directive on the basis of which the LPW could be improved. It is foreseen that each country must report on the implementation of the Directive, that is, the acts on the basis of which it was developed, as well as statistical data. Data is collected on reports, investigations initiated on the basis of those reports and financial effects. In Serbia, not only is the preparation of such a report not regulated by law, but the preconditions for it have not been created either. Authorities and legal entities that apply the Law do not have the duty to keep records.

The EU also foresaw that, based on the data obtained, it will consider the implementation of the Directive and the need for its improvement. LPW did not envisage a similar obligation for the Ministry of Justice or for the Government and the National Assembly.

Article 28

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 29

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 23 October 2019.

For the European Parliament
The President
D. M. SASSOLI

For the Council
The President
T. TUPPURAINEN

Certain weaknesses of the Law on the Protection of the Whistleblower

DEFINITIONS

Title and subject

LAW ON THE PROTECTION OF WHISTLEBLOWERS

> The title of the Law would be more complete if it included the other, equally important, matter to be regulated – whistleblowing. In practice, it is evident that, due to the title of the Law, (but certainly not just because of it) the effect analyses of Law implementation give **disproportionate importance to the protection of whistleblowers and the act of whistleblowing, for which this protection was introduced in the first place**.

Article 1

Scope of Law

This Law governs whistleblowing; the whistleblowing procedure; the rights of whistleblowers; the obligations of state authorities and other bodies and organisations and legal entities and other natural persons in relation to whistleblowing; as well as other issues of importance for whistleblowing and the protection of whistleblowers.

> Article 1 includes a customary and objective overview of the most important issues regulated by this Law. It is not uncommon that sanctions are omitted from that list.

The concept of whistleblowing

Article 2

The meaning of the term

For the purposes of this Law, the following terms have the following meanings:

1) "Whistleblowing" shall mean the disclosure of information regarding an infringement of legislation; violation of human rights; exercise of public authority in contravention of the purpose it was granted; or danger to life, public health, safety, and the environment; or with the aim to prevent large-scale damage;

Comment:

> Whistleblowing is defined as disclosure of certain information. In linguistic terms, this implies that the information has not been known previously. However, the remaining provisions of the Law neither elaborate, nor resolve this fundamentally important issue. The potential risk lies in the fact that **the whistleblower does not know whether the information they intend to disclose will also be new to those whom they address**. If they addressed someone who was already familiar with

the information, then there is no "disclosure" in the true sense of the word, but only a "delivery of information". Therefore, the question is whether such cases should be regarded as whistleblowing and whether the protection of whistleblowers should be provided.

The definition does not include the essential element of compliance with the rules of disclosure of information prescribed by this Law. On the other hand, these rules exist, both in terms of the form, and the content of disclosed information. Thus, among other things, Article 5 stipulates that "whistleblowers are entitled to protection, in accordance with the Law... if they disclose the information to their employer, competent authority, or the public, in the manner prescribed by Law". Due to the fact that the definition does not include the element of legality, **two categories of whistleblowing have been created – legal and illegal, as well as two categories of whistleblowers – those who enjoy the protection of those who cannot be protected**. The fact that the society is still developing a positive perception of whistleblowing and whistleblowers is inconsistent with the fact that the Law does not provide protection for some whistleblowers.

Whistleblower

2) "Whistleblower" shall mean any natural person who performs whistleblowing in connection with his employment; hiring procedure; use of services rendered by public and other authorities, holders of public authority or public services; business dealings; and ownership in a business entity;

Comment:

Definition of the term whistleblower shows that **the Law has been improved compared to the models of labour law and international conventions, as well as the willingness for these improvements to be completed**. The result is a compromise that has not been properly explained.

In one of the reports from the public hearing, the Ministry of Justice pointed out that the scope of protection provided by the Law is now wider than what is stipulated by relevant international documents, so "it would not be suitable to abandon such a decision without well-founded analysis and comparative legal examples". Similarly, the Government and MPs commented on the proposed amendments in this area during the parliamentary debate, with some of them even claiming that changes to documents would be contrary to the documents of the Council of Europe.

It is undoubtedly true that a comparative legal analysis would reveal numerous examples of conditioning, in cases where laws require the existence of some form of association between whistleblowers and bodies where a violation of the public interest took place. However, this is the outcome of historical circumstances, and in particular the fact that the protection of whistleblowers was developed within the framework of labour law regulations. Similarly, the minimum international standards that indicate the condition of being employed or having other similar association with the employer to obtain the protection, and are not intended to exclude other persons from the protection, but to provide protection in areas where retaliation against whistleblowers could usually be expected.

The Law leads to illogical consequences. Imagine a situation where a job tender was not carried out according to the law. This irregularity is indicated by three persons – a job applicant, an employee of this state body, and a student monitoring the job tender for the purpose of writing a term paper. After the whistleblowing, the state body retaliates against all three of them – the job applicant is unfoundedly denied; the employee is demoted to another position; and the student's application for internship is denied a year later. Based on the provisions of the Law, the job applicant and the employee would obtain the protection: the applicant is entitled to protection because the whistleblowing is related to the recruitment process, and the employee would have the same entitlement because the whistleblowing is in some way related to his work engagement (as it is related to the same employer). The student would be left without legal protection, because his or her act was not covered under any of the grounds mentioned in the definition of whistleblowers. All three persons pointed out the same illegality and aimed to act in the public interest, they all suffered damage caused by the same person, but only in the first two cases the Law actually protects the whistleblowing.

Therefore, **there are persons who perform whistleblowing** (e.g. disclose the information about violations of regulations), **and who are not whistleblowers** (do not have a stipulated relationship with "employer"). **Then, there are the persons who perform whistleblowing and who can be whistleblowers, but who are not entitled to legal protection** (for example, due to the breached deadline). Finally, **there are persons who perform whistleblowing, who can be whistleblowers, and who are entitled to legal protection**. All this can create confusion and ultimately negatively affects the popularisation of whistleblowing and whistleblowers.

The status of whistleblower cannot be acquired permanently – it is dependent on the subject of whistleblowing and/or (the Law is unclear) the time when it took place. If an employee A was under a fixed-term contract in a company B, he or she can undoubtedly be granted a whistleblower status when disclosing an illegal action during the course of their employment, and probably after that period, if the illegal action is directly related to their work engagement (but not to any random action of the company B). For example, a patient from a public orthopaedic clinic can be granted a status of whistleblower while waiting for surgery and during the recovery time, and may indicate the negligence of a doctor, a violation of regulations prohibiting smoking, or leaking ceiling. However, according to the Law, they would not be considered a whistleblower if they report illegal procurement of furniture for the office of clinic manager, which they became aware of while recovering from surgery (because it is not related to the service they received from the hospital), nor any other illegal action that took place after their recovery.

A whistleblower may only be a person who performs whistleblowing in connection with their work engagement, use of services, etc. Therefore, a daughter who reports an unlawful action in the case in which the client is her mother, cannot be a whistleblower.

According to the Law, the status of whistleblowers is exclusively granted to individuals. In practice, whistleblowing is sometimes performed by legal entities (citizens' association, company, media founder). These legal entities can undoubtedly suffer consequences because of such actions, and their scope can be much greater than those suffered by an individual whistleblower – (termination of contract on business cooperation, denied funding for programs and projects, boycott). However, even though their whistleblowing is in public interest, according to the Law. Only in the instance in which a natural person was thought to be a whistleblower (either from an association, company, or the media) cloud the protection from retribution said association, company or media has suffered be sought, as the associated party.

The legal definition includes people who are most likely to perform whistleblowing and are most likely to suffer damage. This is actually the additional reason why the stipulation of the condition of prior association seems redundant. One thing is certain – if these conditions did not exist, protection of whistleblowers would be simpler, because there would be one fact less to determine and prove in order to exercise one's rights.

Employer, responsible person, and work engagement

3) "Employer" shall mean any authority of the Republic of Serbia, provincial or local self-government unit, holder of public authorities or public services, legal entity or entrepreneur employing one or more persons;

Comment:

The term "employer" is also important for several reasons. From the standpoint of "employers" and supervision of Law application, it is essential to determine who has the obligation in the case of whistleblowing. From the standpoint of potential whistleblowers, the identification of "employers" is essential to determine whom to turn to perform a legal "internal whistleblowing", as well as to determine if the status of whistleblowers can be granted.

The term **"employer"** is inappropriate and different in meaning from the parent law in which it is used (Labor Law). **It implies authority, legal entity, or businesses** (companies and entrepreneurial activities) in which/where a violation of public interest took place. The truth is that the authorities, legal entities, and businesses are also someone's employers. However, this association will be evident only in some cases of whistleblowing. When whistleblowing is performed by a user of the services of

authorities, an owner of company shares, or a business associate in any of these, then whistleblowing is not considered as performed in relation to the employer (in the linguistic sense), but with the "employer" (in the legal sense).

4) "Responsible person" shall mean any person who is entrusted, in a legal entity, with certain tasks related to management, business operations or business processes, or any person in the state, provincial or local self-government unit engaged in certain activities;

5) "Employment" shall mean full-time employment, work outside of employment, volunteering, exercise of official duty, or any other factual work performed for an employer;

Competent authority for external whistleblowing

6) "Competent authority" shall mean any national, provincial or local self-government authority or holder of public authority competent to act upon information disclosed in accordance with this Law;

Comment:

Just as the term "employer" is essential for internal whistleblowing, the term "competent authority" is important for proper external whistleblowing. In some cases, addressing either "employer" or "competent authority" is a requirement for obtaining protection, hence the importance of knowing who the authority is. Even though this is not particularly emphasized, **several competent authorities can be responsible for "acting in accordance with the information"**. Quite possible are the situations where an authority is responsible for acting upon only one part of the "information", and another authority acting upon a different part. Finally, it could be expected that, in many cases, it would be unclear which authority is responsible for acting, due to ambiguities of the "information" itself.

This is also an example of an incorrectly chosen term. As it can be seen from the definition, the term actually implies a "competent authority" responsible for acting in relation to a problem indicated by a whistleblower. In other words, this definition essentially implies that the "competent authority is ... the authority responsible for acting". Since neither this section (nor other sections of the Law) stipulates who the "competent authority" is, or the manner of determining the competent authority in case of doubt, it appears that this definition was unnecessary. In either case, whistleblowers will have to examine other regulations to find out who "competent authority" is, as this Law and the regulations made thereunder do not provide such an answer.

Damaging action

7) "Damaging action" shall mean any action or omission in relation to whistleblowers which violates or infringes the right of a whistleblower or persons entitled to protection as a whistleblower, or which puts such persons at a disadvantage.

Comment:

Some situations may involve a dispute over whether the right of a whistleblower was violated by an action undoubtedly harmful for them. For example, a citizen who previously acted as a whistleblower is entitled to be issued a license by the competent administrative authority within 15 days, if all the requirements have been met. The citizen has an interest for the license to be issued earlier, but not the right to request the competent authority to do so. Damage could be inflicted if the citizen was not issued a license until the fifteenth day, although the competent authority was able to do so earlier. Because of such cases, **it would be good** if the definition was broader, and **if damaging action included endangerment of one's interest in addition to endangerment of the rights**. This is particularly important in situations where the manner of exercising a right is not sufficiently regulated, or when the right is not precisely defined.

The term "placing someone at a disadvantage," could be interpreted as "placing someone at a disadvantage *as a result of whistleblowing*", or "*in connection with whistleblowing*", as contained in other provisions of the Law. If this term was interpreted without the latter provisions, it would be possible to deduce different interpretations ("placing someone at a disadvantage *in regards to other persons in a similar situation*"). The first interpretation implies a certain level of knowledge about the motives of the person causing damage to whistleblowers. This potential problem is solved by the latter standards which set out the rules on burden of proof. The second interpretation allows for the impression of "placing someone at a disadvantage" to be made credible in a much easier and objective manner. However, it can also lead to a dead end if there are no "*others*" who were treated in the same way, and who could be compared to whistleblowers. For example, a whistleblower is the only person who was fired on the grounds that the position was no longer needed, and the only person who was performing such a function in the entire company. If we accept the first interpretation, the comparison of equal treatment (towards whistleblowers and others), this can be used as a means to determine whether the damaging action was related to whistleblowing.

POSTULATES

Prevention of whistleblowing and performing damaging action

Article 3

Prevention of Whistleblowing Prohibited

Prevention of whistleblowing shall be prohibited.

Any provision of a general or particular enactment that prevents whistleblowing shall be null and void.

This article stipulates a fundamental prohibition of the prevention of whistleblowing and very strict consequences in the event that some general or individual act of whistleblowing was prohibited.

In the opening sections of the Law, whistleblowing is defined as "disclosure of information" on the violation of regulations and other damaging actions listed, but without the elements of legality. The remaining provisions of the Law stipulate the procedural and substantive grounds used for providing legal protection for some types of whistleblowing, and not for the others.

This creates a problem with the provisions of Article 3 of the Law, prohibiting not only the prevention of "good whistleblowing", but also the "bad" one. Moreover, preventing illegal whistleblowing is also the duty of state authorities. For example, the police are obliged to maintain the confidentiality of information on criminal investigations until the investigations are concluded. The problem of information leakage is recognized as important even in the negotiating chapters (23 and 24) with the EU and solutions for this issue are being sought. On the other hand, according to the Law, a situation in which a police officer publicly discloses an information about an ongoing investigation meets all the requirements to be called "whistleblowing" – it refers to the discovery of "information" concerning the violation of the law (criminal investigation is related to criminal offenses). Such negligent police officers would not receive legal protection as whistleblowers. However, any action of the director of the police that would aim to prevent the disclosure of information about the investigation would present "an action that prevents whistleblowing" and as such would be void under Article 3, paragraph 2 of the Law. This was certainly not the intention of the legislator, but no actions have been taken to correct this. Government's explanation for declining the amendment that intended to rectify this issue states "it is a norm of a general character stipulating the rule of prohibiting the prevention of whistleblowing".

Article 4

Damaging Actions Prohibited

Undertaking any damaging action shall be prohibited.

The conditions for the protection of whistleblowers and the issue of conscientiousness

Article 5

Entitlement to Protection of Whistleblowers

A whistleblower shall be entitled to protection in accordance with this Law where:

1) He performs whistleblowing by disclosing information to his employer, competent authority, or the public as provided for herein;

2) He discloses information referred to in Article 2, item 1 hereof (hereinafter referred to as: the disclosure) within one year of having learned of the performance of the action he blows the information for, and at the latest within ten years from the date of the performance of such action;

3) At the time of whistleblowing, the truthfulness of the information disclosed would be credible to a person possessing the same average level of knowledge and experience as the whistleblower.

Comment:

Subjective deadline is one year of becoming aware of the "performed action", and objective deadline is ten years after the event. Deadlines are clearly defined. However, this does not imply that the manner of their practical application, or the purpose of their designation, will always be clear.

Subjective deadlines can be interpreted in a "subjective" way. Therefore, it could be questionable whether a whistleblower discovered the information within the deadline, or if he or she were already familiar with some of the events in question. The whistleblower would then have the right to argue that only the discovery of the most recent information revealed the actual "action" they wanted to disclose. Another option is for the subjective deadline to be perceived in an "objective" way, from the moment the information first became available to the whistleblower (e.g. when they gained access to a harmful contract). In that case, the defendant could challenge in court the legality of whistleblowing, presenting evidence that the whistleblower had knowledge about that event for one year.

Article 4 of the Law on the protection of whistleblowers introduced the term "action", which aims to embrace everything that can be a subject of whistleblowing (e.g. law violation, endangering one's health, and so on.). It would be better if that term had already been included in the definitions, and it also does not seem to be the best possible choice as some cases do not involve any kind of action (taken by a person), but an occurring event (e.g. a crack in a load-bearing wall). An "action" can also include a failure to do something, which can lead to danger for public health for instance.

Things get complicated if a whistleblower discloses several problematic actions at the same time, some of which have occurred within the period of one year/decade, and some before that. The whistleblower would then undoubtedly enjoy protection in relation to *one part of the information* that was disclosed. However, the person taking retaliation against the whistleblower could justify their actions by saying they refer to the other part of "information" that does not enjoy legal protection, and not to the one covered by the deadline, concluding that the complaint should be rejected as inadmissible.

The logical question is – what are the deadlines set in the first place? They (e.g. statute of limitations, deadlines for filing lawsuits) are usually set so that the courts and other state bodies could deal with the issues that are more urgent and socially relevant. This could be an explanation in this case – why would the employers, competent authorities, and courts deal with something that took place more than ten years ago, when it is more productive to get engaged in new challenges. Another

possible reason for setting deadlines refers to the conscientiousness of a whistleblower. Perhaps the legislators felt that it would not be appropriate to protect someone who discovers a disputed action and then waits for two or five years to disclose it (for example, to prevent being justifiably prosecuted for something else). Preambles of the Law did not provide a clear answer as to why these deadlines exist.

Conditioning whistleblowers to reveal information within one year of the discovery is equally arguable. If the aim of the Law is to disclose information about harmful actions and events, it is more logical not to prescribe such a general deadline, but to provide protection to the whistleblowers who planned the time of disclosure/reporting, no matter how much time has passed. If, however, such behaviour is deemed unethical, then the one-year deadline is too long.

A very important standard part of the conditions in international documents and some foreign laws that allow certain actions to be recognized as whistleblowing refers to the so-called "good faith" or conscientiousness of whistleblowers (the Law does not use either one of these two terms). Although the terms are not specifically mentioned, conscientiousness is referenced in the Law only in regards to truthfulness of the information, or, more precisely, the belief in the truthfulness of the information. The disclosed "information" does not necessarily have to be true in order for a whistleblower to receive protection. This simplifies whistleblowing and protects whistleblowers from the obligation to perform checks in regards to what might put them at risk. In the end, the truthfulness of any suspicions and allegations is usually determined in a procedure that is initiated after whistleblowing.

The criterion was set "objectively". No matter how unusual it may seem, there is no investigation if the whistleblower believed in the truthfulness of the disclosed information, but whether "a person with average knowledge and experience comparable to that of whistleblower" believed in the veracity of the information. This assessment is based on data that was available to the whistleblower before disclosing the information. Since a person can have "average knowledge and experience" or "knowledge and experience comparable to that of a whistleblower", but not both, there is only one logical interpretation of such condition: **examining if a person with average knowledge and experience comparable to that of whistleblower would believe in truthfulness of the information on the basis of available details**. This interpretation refers to a hypothetical person who may not testify in the protection of whistleblowers, so in practice, the fulfilment of this condition is determined by questioning the whistleblower or using the court's estimation on how a hypothetical person would reason.

The outcome of criteria objectivity is that a whistleblower may be conscientious and believe in the truthfulness of the disclosed information, yet does not receive protection. This could happen if the court decides that a person with average knowledge and similar experience as a whistleblower recognized that information as untrue. On the other hand, a whistleblower may be negligent and knowingly disclose the disinformation, but obtain legal protection, if a person with "average knowledge" and similar experiences such as whistleblower believed in the truthfulness of the information. These are unfavourable and undesirable consequences of the formulation used by the legislator.

The term "truthfulness" is not further defined by this Law, which causes dilemmas as to whether this condition is being met. For example, such dilemmas may arise in connection to the question of whether the complete information was submitted (in other words, was there a belief that the "information" was true if the whistleblower, who was in possession of the entire document, revealed only one part of it, thus raising the suspicion of law violation, but not revealing the part that lifts such suspicion); whether the "information" was true if the document used to draw a conclusion on the violation of regulations, harm, or danger was replaced by a new document, which whistleblower was aware of (i.e. a harmful contract which has been amended by the annexes that made it acceptable). Finally, another important question is **what exactly needs to meet the requirement of truthfulness – is it only a certain suspicion or allegation explicitly stated by a whistleblower, or is it a document composed or submitted by a whistleblower?** The mere act of whistleblowing often does not consist of presenting suspicion, but of releasing documents or other evidence based on which it can be concluded that a violation of the rules or danger to the public interest took place.

The Law does not completely exclude offering protection to the whistleblowers who act as extortionists. Here we are required to differentiate two things. They are required legal protection from whistleblowing, which protects them from, amongst other things, taking legal action against them "for being a whistleblower". However, a legal course of action could be taken against them for other reasons, amongst which is extortion and blackmail. In these situations, in which a person

is provided legal protection and presents himself in a positive light, as a whistleblower, on the other hand is being prosecuted for a serious criminal offense in connection to and preceding the sole act of whistleblowing, is ultimately bad. In this sense, the main question is will the number of potential whistleblowers with "pure intentions" want to be" thrown in the same basket" as those who committed extortion for their own personal gain.

The risk to public interest is also reflected in the situations of initiating separate system of legal protection of persons who, according to the Law, are whistleblowers, but the significance of violations of regulations they point out to is very small. Just as there is a "small claim crime", or the situation in which, due to a very small value of the committed theft, criminal prosecution is not initiated, it is worth considering whether it is justified to switch the burden of proof claiming that the "damaging action" in connection to the information disclosed by a whistleblower is of little significance.

For example, someone who "discloses" that their boss or colleague lit a cigarette in an empty office next to an open window will enjoy the same legal protection as someone who discloses the threat to the health of a large number of citizens, or a large-scale corruption. The risk of such a legal concept diminishes the newly introduced concept of whistleblowing. Moreover, an additional risk to the system would be caused if the whistleblowing results in completely opposite effects and becomes a means for harassment, rather than the protection of public interest. A possible solution to this risk would be the distinction between cases of illegal actions whose disclosure always presents the endangerment of public interest (e.g. crimes, offenses punishable by a maximum fine, endangerment of public safety and health, etc.), and the cases in which the protection is provided only to whistleblowers who disclose a serious or consistent breach of regulations (as opposed to a slight and sporadic one). Undoubtedly, such a set of rules would create other risks – e.g. whistleblowers may become reluctant to disclose an illegal action because they do not know if they meet the criteria for protection, or may have dilemmas in assessing whether those criteria were met.

PROTECTION OF PERSONS WHO ARE NOT WHISTLEBLOWERS

Associated Persons

Article 6

Protection of Associated Persons

An associated person shall enjoy the same protection as a whistleblower if such person makes probable that a damaging action has been undertaken against him due to his connection to a whistleblower.

Comment:

> "Associated persons" have to "make probable" the interpretation that a harmful consequence was an outcome of "information" disclosure. The Court makes a decision whether to consider such interpretation as probable. In addition, "associated persons" are also responsible for proving association with whistleblowers. It seems that one of the main questions in these disputes could be (absence of) knowledge of the defendant as to whether the "associated person" was in connection with a whistleblower. In such situations, defendants could possibly try to defend themselves by claiming that no retaliation was performed towards the "associated person" because they were not aware of the connection with the whistleblower.

Non-whistleblower

Article 7

Entitlement to Protection due to Wrongful Identification as Whistleblower

A person who makes probable that a damaging action has been undertaken against him, due to the fact that the person performing the damaging action wrongly believed that person to be the whistleblower or an associated person, shall enjoy the same entitlement to protection as the whistleblower.

Comment:

> Also interesting is the legal provision on the protection of "wrongly identified" whistleblowers, and "wrongly identified" associated persons.
>
> It may be difficult to prove this kind of (absence of) whistleblowing.
>
> An interesting question is whether this policy can be applied not only in cases where someone is wrongfully identified as a whistleblower, but also when it is questionable if any type of whistleblowing took place at all. It can happen that someone wrongfully believes that whistleblowing took place and starts looking for the "culprit". For example, a shop owner who was unexpectedly visited by inspection can suspect that control was caused by a complaint of one of the employees for violating the regulations on proper food storage, while, in fact, the control was performed on a random sample of town stores.

Performing Official Duty

Article 8

Protection of a Person Performing Official Duty

A person who has discharged the information while performing his official duty shall enjoy the same protection as a whistleblower, if he makes probable that a damaging action has been undertaken due to discharging his official duties.

Comment:

Article 8 of the Law, which was supposed to regulate the protection of officials who act as whistleblowers, brought confusion. This confusion was only alleviated, but not eliminated, by setting more precise specifications during the parliamentary debate.

Given the stipulation that a person who discloses the information while performing an official duty is entitled to protection "as a whistleblower," it can be assumed that the legislature intended to exclude these cases from the concept of whistleblowing. However, **disclosure of "information" by a public official, while performing an official duty, undoubtedly presents an act that falls under the legal definition of whistleblowing**. For example, when a police officer examines a crime scene and writes a criminal complaint against the driver of a public transportation vehicle who caused serious traffic accident, the officer "discloses the information" about "violations of regulations," "in connection with his or her work engagement" because writing such reports is the officer's job. Due to inconsistencies between Article 2 and Article 8 of the Law, officials enjoy parallel protection on two grounds in connection to the disclosure of the same damaging action.

If we also interpreted what was written, indented to be written, or omitted in the officer's report, the following scenario would have happened: officials may enjoy the status of whistleblowers, as well as anyone else, when they do not perform official duties, or when they disclose the information that is not related to their official duties, but for example, their work environment. If the officials who "disclose information" perform official duties, they may not enjoy the status of whistleblowers; and in such cases they enjoy the protection "as whistleblowers" if damaging action was taken against them.

What are the consequences of such norms? When someone is a whistleblower, that person must meet the requirements of Article 5 of the Law, in order to obtain the protection – to address the required parties, to act within a deadline, and to meet the standard of probable veracity of the information. On the other hand, when one enjoys protection "as a whistleblower", the do not have to fulfill any additional conditions, and it is sufficient that, as in this case, they "submit information" and make credible that damaging actions were taken against them as a result of that. Of course, in order to file a complaint under this Article of the Law, that person first has to prove that he or she performed an official duty in this particular case.

Special attention should be given to consideration of the status of public officials and damaging actions that can be taken against them. Thus, for example, a state auditor, in the exercise of their function, indicates unlawful acts of budget beneficiaries (e.g. a ministry). Then the MPs of the minister's political party may launch an initiative for the dismissal of the auditor, relying on some other basis that already existed before, but has never been mentioned. Or, MPs can retaliate and decide not to renew the mandate of the auditor. The auditor could use the Law on the protection of whistleblowers to make a claim that a damaging action was performed against them, because they indicated the violation of the law, while carrying out official duties. **In such cases, the court would not be able to provide protection from damaging action** (which is otherwise stipulated under the Law on the protection of whistleblowers) **because the damaging action is performed by MPs who exercised their constitutional powers.** The question remains whether the court could prevent taking damaging action against the official if such action was performed under the authority of lower legal acts (e.g. Government's decision by which the auditor is denied the right to use the company car).

Information seekers

Article 9

Entitlement to Protection for Requesting Information

A person requesting data in relation to the information shall enjoy the same protection as a whistleblower, if such person makes probable that a damaging action has been undertaken against him due to requesting such data.

The outdated alert cases, not followed by appropriate actions of government bodies or disclosed information on the taken measures, arouse public interest. A government aiming to hide its poor work, or an official aiming to avoid responsibility, have a motive to silence those who ask questions. This is the probable reason why this standard was added to the Law without any explanation. However, the visible result leaves some doubts and risks. First, **when it comes to "requesting information" a possibility was left for this term to be interpreted in a very limited way, as a request for the document that was submitted to an "employer" or an "authorised body" at the time this Law was in force**. This would, for example, be the case of requesting copies of criminal charges or complaints.

Next, a broader interpretation would be that any request for data on actions or events that could be the "information" is protected, i.e. the data on any irregular or damaging action (as defined in Article 2 of the Law), regardless of whether they originate from a whistleblower. This might be the information established by a state authority or a public service – e.g. information about the increased pollution of water and air.

Even broader interpretation, for which there is no legal support, would be to provide protection for people who seek information that could be used for obtaining the status of a whistleblower. For example, if someone is collecting data on mortality rate from specific disease over a period of time, as well as the data on the emission of exhaust gases in the area, so that these could be used later to alert the relevant authorities should any correlation between the two be found. The report of the public hearing argued that this was the precise objective of this norm: "This formulation embraces all activities of potential whistleblowers with the aim of discovering information. These activities are not considered whistleblowing, but if the person makes credible that he or she suffers damage as a result of it, they can be protected as whistleblowers. In addition, this provision also includes a situation when a potential whistleblower seeks legal advice. Such activity does not present whistleblowing in terms of the Law, but it can be protected if the person suffers damage because of it. "While it is good to have this interpretation in mind as a reflection of legislator's intentions, it is not adequately transformed into legal norms. Seeking information for future whistleblowing does not always imply the request for data related to the "information". A "potential whistleblower" still does not know whether they will really find something that constitutes a violation, or something suitable for performing whistleblowing.

Additional question is whether the protection would be provided in case of requesting data on the acts upon "information", and not only the data "related to information" (as such). Possible interpretations on all these issues determine if the seeker of information will be given protection "as a whistleblower."

On the other hand, provision of protection also includes risks. **Although a request for information on a disputed event deserves legal protection, such a request can be executed along with the violation of another law**. For example, along with the request for disclosure of data, the prosecutor can also publicly disclose personal information of third parties, false accusations of criminal offences, and similar details. The prosecutor should not be entitled to protection in relation to these actions. Judging by the responses of the Minister during the assembly debate, it seems that the intention is not to provide such protection, but for whistleblowers to be held responsible for possible violations of other laws, and in accordance with the provisions of these regulations.

Unprotected reluctant whistleblowers

Comment:

At this point, we would like to remind of the proposal to amend the Law with a special Article aimed to protect "reluctant whistleblowers" – people who were entrusted with the "information", without their intent to address "employer", "authorised body" or "public". The proposal was not accepted in the public debate and parliamentary discussion.

A reluctant whistleblower may be someone who discovers the information in the "relationship of trust", which is based on respect for the rules of professional ethics and protected even in the case of disclosing the information on criminal offences (confession to a priest, doctor, or lawyer, constitutionally guaranteed secrecy of documents). In the event that the unrelated person becomes aware of the secret information, protection from retaliation should be provided. The right to compensation from the person who violated confidentiality is already protected under other laws.

Study participants whose confidentiality was violated are in a similar position.

PERSONAL DATA AND THEIR ABUSE

Protection of Whistleblower's Personal Data

Article 10

Protection of Whistleblower's Personal Data

A person authorised to receive the information shall be required to protect the whistleblower's personal data and any data that may be used to discover the identity of the whistleblower, unless the whistleblower agrees to reveal such personal data in accordance with the law regulating personal data protection.

Any person who learns about the data referred to in paragraph 1 of this Article shall be required to protect such data.

A person authorised to receive the information shall be required to, at the time of receiving such disclosure, notify the whistleblower that his identity may be revealed to a competent authority if actions of that authority cannot be undertaken without revealing the identity of the whistleblower, and notify the whistleblower of the safeguards available to participants in criminal proceedings.

Where it is necessary to reveal the identity of a whistleblower in the course of proceedings, the person authorised to receive the information shall be required to notify the whistleblower of this fact before revealing the whistleblower's identity.

Data referred to in paragraph 1 hereof may not be revealed to any person named in the information, unless otherwise provided by other law.

The first paragraph of this article **introduced the assumption that whistleblowers do not want anyone to know about their acts**. Personal data of whistleblowers (name, address, etc.), as well as the data that could reveal their identity (e.g. cell phone number, IP address or email address) must be protected until whistleblowers agree otherwise.

This is one of the meeting points between the Law on the protection of whistleblowers and other laws, which may cause a dilemma about proper implementation. The provision of the Law on the protection of whistleblowers stipulates for the consent of whistleblowers for disclosure of personal data to be performed in accordance with the provisions of the Law on protection of personal data. In both instances, passing of the legislature provided the possibility of giving written or oral (recorded) consent, or only written consent for particularly sensitive data. However, Article 12 also stipulates the cases of "using the data without consent." **Does the reference to the Law on the protection of personal data imply the possibility of violating the confidentiality of personal data, for the reasons stipulated by this Law?** This would not be logical, as it would imply abandoning the purpose of special regulations on personal data protection of whistleblowers (the Law on the protection of personal data could be applied without doing so). On the other hand, during the discussions on the Law on the protection of whistleblowers, it was repeatedly emphasised that this Law does not take precedence over other laws, and that both Laws are simultaneously applied at their meeting points.

The second Article stipulates the obligation of extending confidentiality to "any person who acquires information". This causes a problem of practical nature – whether any person who acquires the information about whistleblowers will indeed recognize that this is the data that must be kept secret. In regards to the formulation from the related paragraph 1, it is also questionable **whether the obligation to keep the data on whistleblowers secret applies only to cases where the information was first submitted to the "employer" (person authorised for receiving information), or it extends to other forms of whistleblowing**, or to cases where the information was shared with external competent authorities or even with public (and the identity was not known to everyone).

Paragraphs 3 and 4 reference situations where the identity of a whistleblower becomes revealed. Upon obtaining information, the person authorised for receiving such information (again, the only reference is to a person in connection with the "employer", without any reference to a person receiving the information within the relevant external authority) is obliged to inform the whistleblower that their identity may be disclosed to the competent authority under certain conditions. These are the situations where the authority *would not be able to act* without revealing the identity of a whistleblower.

The biggest risk for whistleblowers and a challenge for the implementation of the Law is the question of **establishing situations in which the authorities "would not be able" to take action?** Will this be regarded as a scenario where the authority could conduct the investigation without the data on whistleblowers, which would then become more difficult? In any case, **the opportunity for the violation of confidentiality of whistleblowers' personal data is presented with an inconsistent solution**. At the same time, the Law leaves the possibility of anonymous whistleblowing.

Referencing data on the extent of protection of participants in criminal proceedings may be appropriate in some cases of whistleblowing, but not in all such situations. Therefore, the fulfilment of this legal obligation could also be absurd.

The last paragraph of this Article prohibits the data on whistleblowers to be revealed to the "person indicated by the information." This may be a person indicated as a possible law offender or any other person mentioned in this regard (e.g. a witness, or an accidental participant in the event). As this norm is not precisely defined, different interpretations are possible – more precise would be the formulation "the person indicated by the information as the offender...". Another dilemma is created by the situations when the "indicated person" has not been identified by name, but as a member of a group (e.g. officials employed in certain sectors).

An exception is provided for this rule as well. The data on whistleblowers must also be given to such a person, if a special law provides so. As in all other cases, the stipulations of other laws again take precedence over the Law on the Protection of Whistleblowers.

Abuse of Whistleblowing

Article 11

Abuse of Whistleblowing Prohibited

Abuse of whistleblowing shall be prohibited.

Abuse of whistleblowing shall be deemed present where a person:

1) Discloses information he knows to be false;
2) Seeks illegal gain for himself in addition to seeking action to be taken with respect to the information disclosed.

Comment:

The first kind of abuse recognized by the legislator is the "delivery" of information for which the whistleblower knows that is not true. Interestingly enough, the term "delivery" is used instead of "disclosure" at this point, and it is unlikely to be done intentionally but rather an error on the behalf of the legislator.

The notion of truthfulness is not sufficiently clarified in the Law, which can create problems in its implementation. It could be amended so as to specify that it includes accuracy, completeness, and timeliness. For example, when whistleblowing is performed by submitting a document that indicates a violation of regulations, without any comments from a whistleblower, it will undoubtedly be "true" that the document was drafted and that it indicates a violation of the law. But, it can also be true that the document was subsequently amended and that the illegality was removed (which

the whistleblower was aware of, but did not indicate, nor deliver other documents at their disposal). On the other hand, such specifications could create new problems – some whistleblowers might start wondering if they meet legal requirements and refrain from whistleblowing.

The provision of paragraph 2 is not logical. A person can seek benefit for themselves or another person, regardless of whether they also sought actions to be taken in connection with the information. This can be done by a person who only provided information on the violation of regulations, without making any requests for the violation to be removed. The current provision carries the risk for some abuses, which the legislature intended to prevent, to stay “under the radar”.

The Law states that whistleblowing is abused in cases when unlawful benefit is sought. This benefit may be requested for oneself or another person (not specifically stated). The Law does not provide any related situations, and the question arises if they could be included in the current definition of the term abuse. For example, a whistleblower may seek to cause damages to someone or violate someone’s rights, without benefiting from such actions in any way.

Main dilemmas in the existing text may arise in regards to the **interpretation of the concept of unlawful benefit – whether it refers to any benefit that a whistleblower is not entitled to on the basis of regulations, or only to those benefits whose acquisition would be explicitly prohibited on the basis of a certain regulation?** For example, the Law on the Protection of Whistleblowers does not recognize the practice of awarding whistleblowers who make significant contributions to public savings or revenues. If a whistleblower requests to receive a payment in the amount of 10% of the money that will be allocated to the budget on the basis of information provided, the authority shall not meet such request, since it has no legal grounds. On the other hand, no (other) Law prohibits citizens to submit such requests to state authorities, so it could be argued that these requests are not contrary to the law.

Dilemmas in the implementation of the Law may be considerable when the request is not explicit, but formulated in some indirect way, such as an appeal, expectation, inquiry, or suggestion about additional information, or in cases when the request is related to the award of a social recognition, which authority can always grant to a whistleblower by means of a special decision.

Given the fact that the legality of actions is not a requirement for a certain act to be characterised as whistleblowing, as we pointed out in the comments on definitions, the person who abuses whistleblowing can still be called a whistleblower, based on Article 11 of the Law. Although these abusers eventually do not enjoy legal protection, the mere fact that they are called “whistleblowers” will negatively impact public perception and morale of conscientious whistleblowers.

THE PROCESS OF WHISTLEBLOWING

Classification

Article 12

Types of Whistleblowing

Whistleblowing may be internal, external, or public.

Disclosing information to an employer shall be deemed internal whistleblowing.

Disclosing information to a competent authority shall be deemed external whistleblowing.

Disclosing information to the media, by means of the Internet, at a public gathering, or in any other manner that information may be made public shall be deemed public whistleblowing.

Comment:

This Article defines specific types of whistleblowing (internal, external, and public). The terminology is not completely adequate, because the so-called “internal whistleblowing” is internal only for someone who is a part of that group, for employees, executives, or business owners. For business partners and service users, this is actually external whistleblowing. In such case, whistleblowing is “internal” only inasmuch as being solved within the institution where the problem occurred or has been identified.

In order to properly perform internal whistleblowing, a whistleblower should address the “employer”. Surprisingly, the Law provides little information about which “employer” is “the right one”. In fact, the very definition of “employer” determines only the authorities, organisations, legal entities, and businesses that can be “employers” under the LPW. **The definition**, however, **does not include the criteria for defining the employer that is being addressed by a whistleblower**, and such criteria cannot be found in other provisions either. On the basis of Article 5. Para 1. Item 1. “whistleblowing is performed with the employer...” but there are no specifications on who the “employer” should be. It would be logical if the “employer” was identified, in both terminological and normative terms, as an authority, organisation, or legal person within whose jurisdiction the breach of regulations, endangerment of public interest, or damage took place.

In the absence of other criteria, the “competent” employer can be determined by using a reverse approach – on the basis of relationships (work or other engagement, business cooperation, etc.). **The problem indicated by whistleblowing may be related to some other “employer”, or to a person who does not have this role.** For example, imagine that an employee in the Ministry of Culture in Belgrade was reviewing the documents on the restoration of a monastery, and accidentally found information that indicated that a Municipality in Southwestern Serbia did not obey the Law on public procurement as it failed to pass a mandatory internal act. The adoption of the act is not a question that an official is required to address within the scope of their official duties, and such verification does not fall in the jurisdiction of the Ministry of Culture. If a staff member from this example wishes to disclose this information, and to obtain the status of a whistleblower, they can contact only an authorised person in their ministry, and not the person authorised to act in the municipality where the irregularity took place, or the authority competent to monitor the work of local self-government. The ministry official and the local self-government are not in any relationship that the Law recognizes as a prerequisite for whistleblowing – the official is not employed in this body, does not use the services of a remote municipal government, and does not have business cooperation with this authority. This is one of the absurd consequences of the legal definition that conditions whistleblowing by the existence of some form of prior association between the whistleblowers and the “employer“. The alternative would be even worse –interpreting that the ministry official cannot become a whistleblower at all in cases when he or she is disclosing the information on abuses in the municipality, because this information is not related to “their work engagement.”

In cases of bodies and organisations with complex structures, it can be challenging to determine if an act presents internal or external whistleblowing. Thus, in the context of a public company, addressing the supervisory board essentially presents external whistleblowing, even though it takes place within the same legal entity, because the supervisory board, as an organ of the company, has a certain jurisdiction over the director. Since the Law does not stipulate whether a whistleblower should perform internal or external whistleblowing first, this dilemma has no practical significance for whistleblowers. However, there is a difference from the point of obligations fulfilled by this body. Some of the obligations are related exclusively to the "employer" and the person authorised to receive information, but not to the (external) "competent authority."

The provision related to informing the public is circular – "Alerting the public refers to disclosure of information... to the public ". The term "public" is neither defined in the Law, nor justified in its proposal.

Mandatory Elements

Article 13

Content of Disclosure

The disclosure shall include information regarding any infringement of legislation; violation of human rights; exercise of public authority in contravention of its intended purpose; danger to life, public health, safety, and the environment; or information intended to prevent large-scale damage.

The disclosure may include the whistleblower's signature and data on the whistleblower.

The employer and competent authority shall be required to act, within their respective remits, upon anonymous disclosures.

Article 13 uses these terms in a different way from the introductory definitions. Although it is not explicitly stated, the term "information" used here implies a document (letter, message, recorded note...) in which a whistleblower discloses the "information" (within the meaning of Article 2 of the Law). Such a conclusion is indicated by the provisions of paragraph 1 which stipulates the information that must be included in such a document, and by paragraph 2, which stipulates which information may (but does not need to) be included.

On the other hand, the term "information" in Article 2 of the Law is stipulated as the subject of whistleblowing – "disclosure of information about violations of regulations, violation of human rights, the exercise of public power contrary to the purpose for which it was entrusted, danger to life, public health, safety, environment, and for the purpose of preventing a major damage." In the definitions, **the term information is not identical with the document indicated by a whistleblower when performing whistleblowing.** This document contains the "information" (for example, the description of a crime or violation of human rights), but also includes the other data – e.g. the signature of a whistleblower, or consideration of other issues that the whistleblower brought into connection with the "information".

Of course, it would be far better if other terms that create fewer opportunities for confusion were selected instead of the term "information" in both cases.

The Law does not provide the answer to the question – **whether the submission of notice of an infringement, which is based on another regulation** (criminal charges, the initiative for criminal proceedings, or a petition to the court president objecting the quality of goods sold or services rendered) **should also be considered whistleblowing?** From the standpoint of the legal definition, such address can meet all the requirements to be considered whistleblowing – it discloses the information about an illegal or harmful action to an "employer" or an "competent authority", and there is a legally required type of relationship between an acting person and the body where the violation or damage took place (work relationship, business cooperation, etc.). This question is not just theoretical. On the contrary, when it comes to the form of address, the LPW and other regulations

may come into conflict. The legislator's intentions were not clear enough, so it cannot be said with certainty whether they were properly translated into rules.

Other personal data that may or may not be indicated by a whistleblower are equally important as signatures. It is not possible to provide legal protection for whistleblowers if there is no reliable way to determine that the person performed whistleblowing. This is not possible to do unless a whistleblower provides the information that can be used to establish their identity. On the other hand, if a whistleblower does not provide personal information, there is less chance that they will need protection, that is, that a harmful action will be taken against them. The persons who do not provide such personal information may be exposed to harmful action only if their identity is subsequently discovered, for example, through the investigation conducted for this purpose by the indicated culprit. In such situations, **true whistleblowers may have an interest to deny the fact that they performed whistleblowing**. Not only because they would avoid retaliation, but also because it is much easier to obtain legal protection as a "wrongfully identified whistleblower" than as a true one to which the conditions for providing protection do not apply (deadlines, the veracity of the information, non-conditioning, data secrecy).

"Employer" and "competent authority" **are obliged to act on anonymous complaints in connection with the information, "within their powers". The resulting problem is reflected in the question of the unresolved relationship between the LPW and other laws.** The standard could be interpreted as an employer and a body always being obliged to act on an anonymous complaint, even if other regulation prohibits that (e.g. if there was a provision according to which the body should not act on anonymous complaints). Another possible explanation would be that the company or authority who finds themselves in this situation should act within their powers under other regulations. If the other regulation prohibits acting on anonymous complaints, they will have no obligations to act on whistleblowing cases of this kind.

Another question is **what is meant by acting and at what time shall it be considered that the employer and the competent authority fulfilled this obligation.** In other words, will it be enough if the body takes any action after the whistleblowers' complaint, or will the body be obliged to fully examine the case and take all available measures. It is entirely possible that the obligations of the authority are prescribed by some other act. However, this is not the issue here – the dilemma is **whether the LPW brings any innovations in relation to the obligations that the employer or competent authority would have if this act had never been passed?**

It would be good to prescribe the minimum action required to be taken by the body addressed by a whistleblower. For example, this could be the obligation to verify whether the allegations of infringement or other danger to public interest were supported by evidence, to determine whether a violation actually occurred, to inform the whistleblower about the outcome of the investigation, to initiate the procedure for penalising the responsible parties and providing compensation, etc. Such standards could significantly complement the existing "loopholes in the system," or a number of situations when the authority responsible for acting did not do so using the excuse that the obligations were not strictly regulated.

The issue of the intent to perform whistleblowing and the awareness to act as a whistleblower is not mentioned in the LPW. Several provisions implicitly assume that the whistleblower is a person who is aware of this role (i.e. indicating the perpetrators of violations of regulations or public interest, or signing the "information"). However, none of the definitions or other provisions of the Law require a whistleblower to demonstrate awareness or intention to perform whistleblowing. From the standpoint of protection of whistleblowers there is no difference – a person should be protected from retaliation whether they had the intention to perform whistleblowing or not. However, from the point of the obligation of the employers and the competent authorities, it is very important for them to be able to recognize a public whistleblowing. **The risk for a whistleblowing to remain unrecognised is particularly large when the disclosure of information is performed as a secondary action within a longer notification or other form of address.** For example, submitting the study on public procurements from a previous year to all relevant institutions in Serbia (including the authorities responsible for acting on such cases of irregularities) may represent a "disclosure of information" if the study included some particular cases of violations of the law which had not been known before. If the disclosure of this violation was not the prime objective of the address, but was listed as an example on page 54 of the text, it is neither realistic nor reasonable to request the competent authority to act on such a case of whistleblowing.

Internal Whistleblowing

Obligations

b) Internal Whistleblowing

Article 14

Obligations of Employer

Each employer shall be required to undertake all measures necessary to correct determined irregularities in relation to the disclosure.

The employer shall be required to protect the whistleblower from any damaging action, and undertake any and all measures necessary to terminate a damaging action and remove any consequences of a damaging action.

The employer may not undertake any measures to reveal the identity of the whistleblower.

The employer shall be required to notify, in writing, all persons employed of their entitlements hereunder.

The employer shall be required to designate an officer authorised to receive disclosures and be tasked with pursuing proceedings related to whistleblowing.

Comment:

Despite the provisions of this Article, there are still some unresolved dilemmas concerning the relationship between the LPW and other laws. Thus, the obligation of authorities and companies to take "measures to eliminate the established irregularities" "within their powers" may be interpreted as an obligation to do everything possible (engage all capacities). Another interpretation would be for these bodies to, among other things, decide whether and to what extent to examine specific suspicions of illegality and establish the facts "within their powers". The differences in the outcome of the application of one or the other interpretation can be drastic.

What makes this absolute protection of confidentiality even stranger is the fact that the same law anticipated numerous situations in which it can be possible or even required to disclose the identities of those whistleblowers who formed a relationship of trust with the contacted authority and used their name, but did not want any other party to know their identity.

In order for the whistleblowing system to function well, it is important that potential users are very familiar with it. Therefore, a provision obliging an employer to submit a notice to its employees about their rights stipulated by this Law would be very useful. It would certainly be helpful to prescribe the obligation to release this information on the "employer's" website. The harmful effects of drafting the Law using the perspective of labour law are again evident in connection with this provision – even though the law should equally protect other persons (service users, business associates, small shareholders, and the like), **a notification is sent only to those with a work engagement, and there is no mechanism designed to notify other potential whistleblowers of their rights.** This omission has a significant impact on the fulfilment of one of the objectives the Law was supposed to accomplish, and that was particularly emphasised in its justification – reporting corruption. This phenomenon is documented by the experiences of business partners and users of public sector institutions, and the fact that their preventive notification, even at elementary level (bulletin board, or internet website) is not prescribed as an "employer's" obligation.

Procedure

Article 15

Procedure

An internal whistleblowing procedure shall be initiated by the disclosure of information to an employer.

The employer shall be required to immediately act upon any whistleblowing disclosure and at the latest within 15 days of receiving such disclosure.

The employer shall be required to notify the whistleblower of the outcome of the procedure within 15 days of the conclusion of the procedure referred to in paragraph 1 of this Article.

The employer shall, upon the whistleblower's request, provide him with information about the progress of any and all actions undertaken in the course of the procedure, and enable him to have access to the case files and participate in actions in the course of the procedure.

Comment:

It is logical that employers cannot have any obligation to act if they did not receive the information. However, unconditionally binding the right on the protection of whistleblowers to the delivery (receipt) of the information to the employer may give an advantage to those retaliating against whistleblowers. Such an employer can claim that they never received the information, and that the subsequent action that harmed the whistleblower cannot have anything to do with the fact that the whistleblower (allegedly) submitted such information.

In the contains of the legislation one important question remains unclear – **whether the process of whistleblowing is independent from all other processes that existed previously with the authorities, organisations, and companies, or the processes that would be established in the future, or is the whistleblowing an action that can be performed within another regulated procedure?** The already discussed conclusions on the provisions go in favour of the second interpretation. Thus, the statement of intended whistleblowing is not an element that is required as a mandatory part of the act; the definition of whistleblowing references the discovery of information about specific issues to the employer, competent authority, or public, without prejudice to any aspect or medium that can be used to convey this same information in another proceeding.

If we accept this broader interpretation, which we believe would be closer to what is written in the Law (regardless of whether the legislator's intentions may have been different, as might be inferred from some of the reasons for the rejection of the amendment), this would have a negative consequence. People who use the same legal remedy would have different rights in some instances depending on whether they are eligible to be considered whistleblowers or not.

A significant tool in the hands of whistleblowers, which should oblige "employers" to take internal whistleblowing more seriously, is the power to request and obtain notices on the progress and actions taken in the proceedings, to examine case files, and to "be present at the proceedings." These **powers of whistleblowers are not limited in any way, even though there might be room for such action.** It is easy to imagine situations in which a procedure initiated on the basis of information provided by a whistleblower could disclose some data that indicate whistleblower's culpability in another situation. It would be appropriate to examine this matter and keep potential evidence before a whistleblower is informed about everything, and something like that cannot be performed with any restriction of whistleblowers' right to inspect case files and the actions taken in the proceedings.

Internal act

Article 16

General Enactment of Employer

Each employer with more than ten employees shall be required to adopt an internal enactment governing internal whistleblowing procedure.

The employer shall be required to post the general enactment referred to in paragraph 1 of this Article in a visible location that is accessible to each employee, as well as on its web provided that there are technical conditions to do so.

Provisions of the general enactment governing internal whistleblowing procedure must be consistent with the provisions hereof and the bylaw referred to in Article 17 hereof.

Provisions of the general enactment referred to in paragraph 1 of this Article may not reduce the scope of rights or deny any right to a whistleblower within the meaning of this Law.

Provisions of the general enactment referred to in paragraph 1 herein that is not consistent with this Law or bylaws adopted in accordance with this Law shall be null and void.

Comment:

The adoption of an internal act of whistleblowing is mandatory for all employers with more than ten employees. The labour law character of the Law is also evident in another provision. Regardless of the number of customers or small shareholders who could act as whistleblowers, the authorities and companies with a smaller number of employees will not have to adopt a special act on internal whistleblowing.

The second paragraph stipulates the obligation of displaying this act “in a prominent place” as well as on the website “if technical requirements are met”. **It would be useful if, similarly to the postings in the premises, the Law stipulated the obligation for the rulebook to be displayed both in a prominent place and on the internet**, because it often happens that important documents are published on a website section that is hard to find or reach.

The remaining provisions of this article are redundant. The acts of lower legal power shall not be contrary to the acts of higher legal power. They cannot reduce the scope of the rights or deny any right arising from the law.

Article 17

Enactment of Minister

The Minister in charge of judicial affairs shall adopt an enactment to closely regulate the manner of internal whistleblowing, the manner of appointment of an authorised person within an employer, and any other issue relevant for internal whistleblowing applicable to employers with more than ten employees.

Comment:

On the basis of this authorization, the Minister of Justice issued the *Rulebook on the method of internal whistleblowing, the method of determining an internal whistleblower with an employer, as well as other issues of importance for the internal whistleblowing with an employer who has more than ten employees.* The act was published on the website of the Ministry of Justice on 5 June 2015

http://www.mpravde.gov.rs/vest/9163/pravilnik-o-nacinu-untrasnjeg-uzbunjivanja.php

The Rulebook brought some refinements, along with the number of repetitions of legal provisions. The Rulebook excluded some of the options for reporting illegal acts that have already been used in practice, and could also be used here, given the obligation to act upon anonymous complaints. Thus, for decades some local governments and companies have been using the practice of its beneficiaries to submit written comments on the work of the body into the special boxes provided. In recent years, online applications have been introduced to allow interested citizens to contact the authorities and express suspicion of corruption and other irregularities. However, this method of communication is also not permitted under the Rulebook!

Therefore, the Rulebook specifies legal “submission” by establishing different criteria for determining the time when the information was submitted. For registered mail, the Rulebook introduced a fictional scenario – that the information was delivered when the mail was handed over to the post office. For regular mail, the time of delivery coincides with the actual event. For e-mail, the Rulebook references other laws and regulations on the receipt confirmation. This neglects the main problem with this mode of communication – some legal persons, who are not obliged to do so, do not issue a receipt confirmation for e-mails, as this obligation is not explicitly stipulated by this Rulebook either.

Article 5 contains a description of the receipt confirmation for the information relating to the internal whistleblowing. It is interesting that some elements that are relevant to determine whether the “information” meets the conditions stipulated by the LPW are not listed as required, as well as whether the conditions were met for the whistleblower to enjoy protection (e.g. some connection of the whistleblowers with the “employer”, type of “information”, time of the act or event referred to in the “information”, etc.).

Very important is also the provision according to which the mail indicated to be delivered to the person authorised to receive information and conduct the proceedings related to internal whistleblowing with the employer, or the mail whose packaging reveals such information, may be opened only by an authorised person. Other forms of information delivery are not secured in this way, which could have been done with emails.

The solution according to which the “authorised person” ceases their work after “proposing the measures”, coupled with the fact that these proposals are not binding for anyone, is not good and does not meet required standards. The LPW obliges the employer to complete the proceedings after receiving the information and to inform the whistleblower about the outcome. Surely, it cannot be assumed that the employer has done all that was in his jurisdiction only by establishing recommendations on what should be done, but by actually doing it.

For example, when an employee within the company indicates to the authorised person that a concluded agreement is harmful to the company, the authorised person shall examine these allegations. That examination can lead to the conclusion that the assistant director probably intentionally concluded a damaging contract because he or she had a private interest in the business. The recommendation of an authorised person could be, for example, for the legal department to initiate proceedings for breach of the contract, for the assistant director to be fired, and for the criminal charges to be taken against him. However, “acting on information” does not end here, but only when the proceedings for the breach of contract, dismissal, and criminal charges truly become initiated.

Some important issues that were not clearly defined by the Law, are not regulated by the Rulebook either, so these could be included in future amendments. Among other things, this primarily refers to the manner of fulfilling the obligation of the employer to provide whistleblowers with requested information on case progress, to allow them access to the case, and presence in procedural actions. In addition, the Rulebook could more closely regulate whistleblowers actions in situations where a person authorised to receive the information is in some way involved, or actions in specific situations – e.g. when the information is provided by a beneficiary of the body and not an employee, etc.

Through the Transparency Serbia’s Anti-Corruption Legal Advice Center, we also learnt of the problems that could also be resolved by editing of the Rulebook. The problems are amongst others, the question of selecting the person inside the company who would be responsible for overseeing the proceedings in case of an internal whistleblowing (cases where the person chosen for the position has not enough responsibilities and knowledge for the position) and the matter of conduct and the responsibility in situations where authorized person is unable to perform his duties for the time being.

External Whistleblowing

Article 18

c) External Whistleblowing

An external whistleblowing procedure shall be initiated by the disclosure of information to a competent authority.

Where whistleblowing pertains to employees of the competent authority, the whistleblower shall make the disclosure to the head of such authority; where whistleblowing pertains to the head of a competent authority, the whistleblower shall make the disclosure to the head of the authority directly superior to such competent authority.

The competent authority shall be required to act upon any disclosure referred to in paragraph 1 of this Article within 15 days of receiving such disclosure.

Where the competent authority to which the disclosure was made does not have jurisdiction to act in connection with such whistleblowing, it shall forward the information to the authority vested with such jurisdiction within 15 days of receiving such information, and shall notify the whistleblower of this action.

The authority referred to in paragraph 4 of this Article shall be bound by the safeguards provided to the whistleblower by the forwarding authority.

Where the whistleblower has not approved that his identity be revealed, and the competent authority to which the disclosure was made by the whistleblower does not have jurisdiction to act, it shall, prior to forwarding the disclosure to the competent authority, request approval for doing so from the whistleblower, unless otherwise stipulated by the law.

The competent authority shall, upon the whistleblower's request, provide him with information about the progress of any and all actions undertaken in the course of the procedure, and enable him to have access to the case files and participate in actions in the course of the procedure.

The competent authority shall be required to notify the whistleblower of the outcome of the procedure referred to in Paragraph 1 hereof after the conclusion of the procedure, in accordance with this Law.

Comment:

"Competent authorities", within which "external whistleblowing" is performed, may be numerous, given the responsibilities they have and the complexity of the issues indicated by whistleblowers. However, the main problem for the whistleblowers is the absence of an obligation on the part of employers to publish the information on which external competent authorities are responsible for acting in some typical situations where whistleblowing can be expected to take place.

The rules of address from Para 2 of this Article seem logical at first glance – if a whistleblower suspects that some official in the control body is corrupted, they will address the head of that body; if they suspect that the supervisor is corrupted, they will address the head of the body that immediately supervises that person. However, this logical assumption also includes a lot of confusion and inconsistencies.

In some situations, a whistleblower will not have clearly defined suspicion about the supervisor in a "competent authority", but about that authority as a whole (e.g. because of the long time the authority took to decide on a case). Therefore, it would be good if this possibility was also mentioned. Second, in some situations, the same problem can be solved by several external control bodies (e.g. budget inspection of the Ministry of Finance and the Public Procurement Office). There is no reason for a whistleblower who suspects the Minister of Finance of being corrupted to be referred to a higher authority. The whistleblower should be presented with the possibility to address the other control body – in this case the Public Procurement Office. Finally, if a whistleblower directly addresses a

superior authority, it is not necessary, and often not appropriate, to address the head of the institution, as addressing the body will suffice.

When it comes to control bodies, many situations will already stipulate an obligation to act in a certain way and in a certain time period from the time when some kind of illegal activity or other problem was reported. The question of what would happen when two deadlines are different has not been resolved. An additional problem is reflected in the fact that the body will have different deadlines for acting when the same problem is reported by the citizens who do not have the status of whistleblowers and those who do.

It is unfortunate that the adoption of the LPW was not used to specify the obligations of state control bodies to act in those cases that are not sufficiently regulated by their respective laws. Among other things, it could be predicted that, if it is not in conflict with the obligations established by other law, the inspection body will be obliged to determine the veracity of allegations of infringement, breach of public interest, damage, or other risks referred to in Article 2, item 1) to which a whistleblower pointed out, as well as those within its jurisdiction; to take measures for prevention or elimination of injuries and hazards; to determine who was responsible for the violations and resulting threats; to take appropriate action against the person responsible; to take appropriate action for the compensation of damages incurred due to injuries and danger.

The situation described by Para 4 of this Article is legally and logically impossible. The definition of “competent authority” includes the authority’s competence to act, so it is impossible that the responsible body is also considered incompetent. When we put aside this terminological confusion, we have the solution according to which the authority that received a notification of a violation of some regulation, where the body has no jurisdiction for further investigation, would forward the information to the competent authority. The deadline for such action is the same as the deadline for acting on the information – 15 days. The authority also informs the whistleblower accordingly. However, as this type of whistleblowing requires whistleblower’s consent, it can easily happen that the authority exceeds the stipulated deadline. It would therefore be useful if the deadline for acting on the information was shorter, or if the deadline for forwarding the information was longer.

Paragraph 7 stipulates that the designated authority shall, upon request, provide whistleblowers with the information on the progress and actions taken in the proceedings, and allow whistleblowers to examine case files and attend procedural actions. This obligation is, however, limited by the closing phrase “in accordance with the law”. It could be interpreted as if a whistleblower enjoys these rights, if that is already stipulated by another law. However, in this case, the standard would be redundant, because it would not bring any novelty in the legal system. Another possible interpretation, which would give a meaning to this provision, would be that whistleblowers are entitled to receive notifications, gain insight, and the like, but only in case that this was stipulated by another law (e.g. parties in a proceeding), and whistleblowers are given the status of persons who have such a right.

The same dilemmas arise in connection with the obligation of an authority to inform the whistleblower of the outcome of their proceedings. Since the notification is done “in accordance with the law”, if another law stipulates such a duty, that duty would also exist here, otherwise not. The deadlines stipulated by that other law would be applied (as they are not stipulated here). The third possible interpretation, which would bring a meaningful solution, but is minimally supported by the LPW, would be to interpret the phrase “in accordance with the law” as “if the law does not prohibit so”.

Public Whistleblowing

Article 19

d) Public Whistleblowing

A whistleblower may disclose information to the public at large without having previously disclosed it to an employer or competent authority in the event of an immediate threat to life, public health, and safety, the environment, to causing large-scale damage, or if there is an immediate threat to destroying the evidence.

When blowing the whistle to the public at large, a whistleblower shall be required to comply with the principle of presumption of innocence of an accused, the right to personal data protection, as well as not to hinder the conduct of the court proceedings.

Comment:

It would be useful if another reason was also stipulated as a reason that fully justifies public address without reaching out to other institutions – the disclosure of information that would otherwise had to be released (but it is not). For example, the authorities have to publish on the Public Procurement Portal and their websites the answers to the questions of interested parties in connection with the tender documents. If they do not do so, it is quite reasonable for this information to be published by a whistleblower anywhere else, without addressing anyone within the contracting authority, the Public Procurement Office, or other control body.

Whistleblowers also have the right to address the public in other situations, but then have to meet another condition to be eligible for protection – that they have previously addressed the employer or a competent authority. The law does not impose any further limitations in this regard – a whistleblower can send an email notification to the authorised control authority or the person authorised by the employer, and seconds later send the same information to all media in the country. Such a solution seems unfeasible because it exposes the employer and the control bodies to a pressure even before that is proven as necessary. It would make sense to allow the competent authority a reasonable time to act, after which a whistleblower would be allowed to address the public. Of course, when it becomes evident that the authority is not conducting a proper procedure, there is no reason to wait for the stipulated deadline or any other reasonable time period.

Finally, there are also situations where whistleblowers are forbidden to address the public, either before or after contacting the employer and the control body. These are discussed in Article 20.

The data classified as secret

e) Handling Classified Information

Article 20

Whistleblowing where Disclosure Contains Classified Information

A disclosure may contain classified information.

Any information classified within the meaning of legislation governing the confidentiality of information shall be deemed classified information referred to in paragraph 1 of this Article.

Where a disclosure contains classified information, the whistleblower shall be required to first make such disclosure to the employer; where a disclosure pertains to a person authorised to act upon such disclosure, the disclosure shall be made to the chief officer of the employer.

Where the employer has failed to act upon a disclosure made by the whistleblower that contains classified information within 15 days, or failed to take appropriate action from within its remit, the whistleblower may contact a competent authority.

Notwithstanding paragraph 3 of this Article, where a disclosure pertains to the chief officer of the employer, such disclosure shall be made to a competent authority.

Where a disclosure contains classified information, the whistleblower may not disclose it to the public at large unless otherwise regulated.

Where a disclosure contains classified information, the whistleblower and other persons shall be required to comply with general and specific measures for the protection of classified information stipulated by the law governing the confidentiality of information.

Comment:

When the norms of the Data Security Act intersect the provisions of the LPW, it can be concluded that the **current legal framework generally excludes the possibility of alerting the public in cases of information that contain classified information.** A whistleblower then must contact the employer, and if the employer fails to act within 15 days, then the competent authority should be contacted (it is possible to directly address the external competent authority in case of doubt that the head of the "employer" is also part of the problem). Any other actions would lead to denial of protection under the LPW and possibly to criminal liability.

Particular caution of whistleblowers is needed in situations of dealing with secret data referred to in Art. 3. of the Data Secrecy Law which stipulates that "the classified information does not include the information marked as secret in order to conceal a crime, acts of exceeding one's powers, abuse of office, or other illegal acts or practices of a public authority". A document can be marked as confidential even if it was not intended to be so, if the secrecy was marked in order to conceal a crime. Even if a whistleblower has a strong reason to believe that the secrecy was mislabeled for any of these reasons, they cannot be entirely sure that they will not be held liable after alerting the public, until the competent authority determines that the label of secrecy was abused. **At the time of reaching the decision, a whistleblower will only have the act that already marked the document as secret, but not reliable knowledge about the motives of those who made the decision on such classification.** Only after the label of confidentiality gets revoked, the whistleblower can safely alert the public and enjoy protection, if all other requirements of the LPW have been met.

In connection with the possible ways of terminating secrecy, the Data Secrecy Law does not stipulate the procedure for establishing that the document has already been made available to the public and that the label of secrecy should be terminated accordingly. In the context of possible criminal liability of whistleblowers for disclosing a secret, **it could be concluded that such liability cannot exist if a whistleblower re-discloses a "secret" information that was already "made available to the public" in any other way and by any other person.** On the other hand, it is questionable whether this would be considered whistleblowing, because the information was not disclosed for the first time.

When the LPW was adopted, an opportunity was missed to move things from a standstill in terms of resolving the documents that were mistakenly labelled as secret. Some of the reasons were presented during the parliamentary debate on the submitted amendments. MPs also addressed the amendment according to which alerting the public was absolutely prohibited only in situations where the highest level of secrecy was determined – "national secret", which is established in order to "prevent irreparable damage to the interests of the Republic of Serbia". In all other cases, alerting the public by disclosing secret data would be allowed according to the amendment and under two general conditions – that such whistleblowing does not cause more damage than the damage indicated in the information, and that the objective of whistleblowing cannot be achieved without disclosing the secret data.

Such a change was not accepted by the government "because the solution proposed by the amendment was contrary to the regulations governing data secrecy.

The risk assessment of possible collision of two laws was undoubtedly correct when it comes to situations that should be avoided. In a situation when there is a problem, as it is the case in Serbia with standards on data secrecy, the problem should be solved. It would certainly be better to do so by specifying the rules in Data Secrecy Law, instead in the Law on the Protection of Whistleblowers.

By current practice on the protection in cases of disclosure of classified information, the whistleblowers remained on the same uncertain ground as before the adoption of the LPW.

Paragraph 2 narrows the meaning of the term “secret data” only to the data labelled as secret “in accordance with the regulations,” i.e. the Data Secrecy Law and other relevant regulations. This would mean that the limitations for whistleblowing in cases of using classified information do not apply when a whistleblower is confident that the information is not labelled as secret. However, the question is – what source of information could be reliable?

The provision of paragraph 2 did not solve the problem of unfounded secrecy, but only moved it to the field of application of Data Secrecy Law, where the problem remained unresolved. In fact, **quite possible and probable are the situations where the information is labelled as secret, but a whistleblower has reason to suspect that this was done in accordance with the regulations**, as well as the situations where a whistleblower simply does not know and has no way of knowing whether the labelling of secrecy was initially done in accordance with the regulations, but believes that such information should be shared with others. The provision of the LPW does not offer a solution to such dilemmas of whistleblowers.

According to paragraph 4, a whistleblower acquires the right to address an external control authority (“competent authority”) only if the employer fails to act in accordance with the information within 15 days, if it fails to respond to it, or fails to take the measures within its jurisdiction. **It’s not clear when the deadline for addressing external authority ends, in cases when a whistleblower received a response within 15 days showing that the employer acted in some way.** The reason to address the competent authority is then created by the failure to take action within the jurisdiction of the employer. If the deadlines for the employer to take certain measures are stipulated elsewhere, that may also be relevant here. However, if the deadlines for taking such measures are not stipulated, the matter can be interpreted as if a whistleblower may address an external authority immediately or completely opposite – that they can never address such an authority.

HOW TO PROTECT WHISTLEBLOWERS?

Putting whistleblowers “at a disadvantage”

Chapter IV

PROTECTION OF WHISTLEBLOWERS AND COMPENSATION FOR DAMAGE

Article 21

Putting Whistleblowers at a Disadvantage Prohibited

The employer of a whistleblower must not perform an action or omit to perform an action that would place a whistleblower at a disadvantage, in particular in relation to:

1) Hiring procedure;
2) Obtaining the status of an intern or volunteer;
3) Work outside of formal employment;
4) Education, training, or professional development;
5) Promotion at work, being evaluated, obtaining or losing a professional title;
6) Disciplinary measures and penalties;
7) Working conditions;
8) Termination of employment;
9) Salary and other forms of remuneration;
10) Share in the profits of the employer;
11) Disbursement of bonuses or incentivizing severance payments;
12) Allocation of duties or transfer to other positions;
13) Failing to take measures to provide protection from harassment by other persons;
14) Mandatory medical examinations or examinations to establish fitness for work;

Provisions of a general enactment denying or infringing upon the right of any whistleblower or placing such persons at a disadvantage shall be null and void.

Comment:

“Putting whistleblowers at a disadvantage” is a form of “damaging action”, but this term has not been defined. Due to the use of comparative forms, **it would be logical to think that this refers to a situation which is disadvantageous in relation to something else** (a position that a whistleblower would have held if there was no retaliation), **or in relation to someone else** (a position that is disadvantageous in relation to other employees, other users, etc.). Numerous “cases” that are listed are not helpful to determine what the legislator wanted to achieve, because they only identified the areas in which someone can be “put at a disadvantage” (e.g. payment of awards and retirement), and not the criteria to determine that the situation is indeed like that.

Paragraph 2 annulled provisions of the general act that deprive or violate whistleblowers’ rights or put them at a disadvantage in relation to whistleblowing. The report of the public hearing lists collective agreement as an example of such a general act. However, the manner in which this annulment would be determined is not clear. The Constitutional Court may suspend the provision of a general act if it is contrary to the law, which could be the case here. However, in proceedings before the Constitutional Court the act cannot be annulled, but only declared unconstitutional/illegal. The Law on Administrative Disputes can annul the acts, but only in case of individual acts. In this regard, it remained unclear why the LPW stipulates annulment only for general acts, and not for individual acts that harm whistleblowers.

Compensation for Damage

Article 22

Compensation for Damage Incurred due to Whistleblowing

In cases where damage is incurred due to whistleblowing, the whistleblower shall be entitled to compensation for damage in accordance with legislation governing contracts and torts.

Comment:

This article of the Law is redundant. Even if this provision was omitted, whistleblowers would be entitled to compensation under the Law on contracts and torts. The provision of compensation for damages would make sense only if this law provided more rights for whistleblowers than the rights guaranteed by the Law on contracts and torts. This might refer to providing guarantees to whistleblowers that they will receive a fair remuneration in any required case, that is, that the court will not make a decision under Art. 185, para. 4. of the Law on contracts and torts on "establishing the former state," even though a whistleblower demanded monetary compensation. This guarantee would be particularly useful for whistleblowers who are facing "silent boycott" in their workplace or other form of retaliation that is difficult to prove. According to Article 185 of the Law on contracts and torts, the responsible person is obliged to restore the former state before the damage occurs. When the establishment of the former state does not eliminate the damage entirely, the responsible person shall make a monetary compensation for the remaining part of incurred damages. When the establishment of the former state is not possible, or when the court decides that the responsible is not necessary in charge of such establishment, the court determines that the responsible person shall pay the injured person an appropriate amount of money as compensation. The court awards monetary compensation to injured persons when such compensation is requested, unless the circumstances of the case justify the establishment of the former state. The amendment aimed to reduce the space for the free assessment of the court granting the requested compensation (instead of reinstatement for example) was rejected as unnecessary "because the Law on contracts and torts regulates the compensation of damages in detail."

The rules of procedure

Article 23

Judicial Relief of Whistleblower

A whistleblower who has suffered a damaging action in relation to whistleblowing shall be entitled to judicial relief.

Judicial relief shall be exercised by lodging a lawsuit seeking protection in relation to whistleblowing with a competent court within six months of learning of a damaging action that has been undertaken, or three years from such time as the damaging action was undertaken.

The court competent to provide judicial relief shall be the high court with territorial jurisdiction over the location where the damaging action was undertaken, or in accordance with the domicile of the plaintiff.

Judicial relief proceedings in connection with whistleblowing shall be urgent.

Appellate review shall always be permitted in proceedings for judicial relief initiated in connection with whistleblowing.

The provisions of the Civil Procedure Code applicable to labour disputes shall apply as appropriate to judicial relief proceedings in connection with whistleblowing, except where otherwise provided for herein.

Trainings

Article 24

Composition of the Court

A single judge shall always try in the first-instance litigation proceedings initiated upon lodged lawsuit in connection with whistleblowing, and the three-judge panel in the second-instance proceedings.

Article 25

Possession of Special Knowledge in Whistleblowing

A judge acting upon a lawsuit in connection with whistleblowing or acting in special circumstances referred to in Article 27 hereof shall be a person who possesses special knowledge in protection of whistleblowers.

Acquiring special knowledge and personal development of persons acting in cases in connection with protection of whistleblowers shall be conducted by the Judicial Academy in cooperation with the Ministry competent for judicial affairs.

Curricula and other related issues of importance for acquiring special knowledge in protection of whistleblowers shall be regulated by an enactment of a minister in charge of judicial affairs.

Comment:

> The training program did not cover all issues that are relevant for whistleblowing and protection of whistleblowers. **The program lacks a more thorough discussion of the application of other regulations that come into contact with the LPW.** The exception is reflected in one part of the training related to the handling of confidential data. In addition, **the time allocated for attending the training is too short** to cover all essential topics.

Lawsuit

Article 26

Content of Lawsuit

The following can be sought in a lawsuit for relief in connection with whistleblowing:

1) Establishment of the fact that a damaging action has been undertaken against a whistleblower;
2) Prohibition of engagement in or repetition of a damaging action;
3) Remediation of the consequences of a damaging action;
4) Compensation for tangible and intangible damage;
5) Publication of the judgement rendered upon a lawsuit filed for reasons referred to in items 1) to 4) above in the media, at the expense of the defendant.

The lawsuit referred to in paragraph 1 of this Article may not contest the legality of an employer's individual enactment adopted to decide on an employee's employment-related rights, obligations and responsibilities.

Comment:

> When the damaging action is taken against employees, this is expected to happen through the adoption of individual acts by employers who decide on the rights, obligations and responsibilities. Therefore, the legal concept in which contesting these acts is exempted from the general regime of the protection of whistleblowers is disputable. Such an exemption would be easier to justify if

the same rule was established for all other legal procedures and in relation to all other individual acts. This seems to be another consequence of focusing on the issue of labour law in protection of whistleblowers, and the fact that the application of other measures for protecting whistleblowers from damaging action was not equally considered when the Law was drafted. Also, this exemption was not justified in the report of the public hearing.

Whistleblowers in labour dispute

Article 27

Rights of Whistleblowers in Specific Proceedings

When lodging a lawsuit to contest the legality of an employer's individual enactment adopted to decide on an employee's employment-related rights, obligations and responsibilities of a whistleblower in accordance with specific legislation, the whistleblower may allege that the employer's individual enactment constitutes a damaging action in relation to whistleblowing.

The allegation referred to in paragraph 1 may be made in the lawsuit or at the preliminary hearing, and may be made at any subsequent point in time only in the event that the alleging party makes it probable that he was unable to make such allegation at an earlier point in time without inculpating himself.

The court shall pursue separate proceedings to decide upon the merit of any allegation whereby the employer's enactment constitutes a damaging action in connection with whistleblowing.

Resolving dispute through mediation

Article 28

Notice to Parties of the Right to Resolve Dispute through Mediation

The court providing relief due to whistleblowing shall, at the preliminary hearing or the first individual session of the main hearing, notify the parties of the option of out-of-court settlement through mediation or in any other amicable manner.

Comment:

This is one of many provisions of the Law whose need has never been justified. In connection with these matters, Article 11 of the LPW (which duly applies to the protection of whistleblowers) already stipulates that "the court shall refer parties to mediation, or to an information session on mediation, in accordance with the law, or indicate the possibility for parties to resolve a dispute in amicable matter or in other agreed way."

From the standpoint of expediency, the stimulation of whistleblowers and employers to settle a dispute in an "amicable" and "mutually agreed" manner, is also questionable. As the court proceedings can lead to disclosure of new information on the violation of public interest, out of court settlement can also be concluded to prevent disclosure of such information.

From the legal standpoint, **any agreement between a whistleblower and an "employer" does not constitute grounds for the exemption from criminal or other liability for violations of the law** – both the subject of whistleblowing, and the action that constituted retaliation. Such an agreement could regulate only the issues that were the subject of the lawsuit – for example, that it is not necessary to take further action because damaging actions have ceased, that whistleblowers will not ask for compensation because they already received satisfaction, and the like. However, it is very likely that the termination of proceedings would lead to the failure to disclose the information on all violations of the employer, and especially to the failure to bring to the attention of the court and other authorities the information on violations of whistleblowers' rights that occurred during the retaliation.

Burden of proving

Article 29

Burden of Proof

In case the plaintiff has, in the course of proceedings, established the probability of having suffered damaging consequences in connection with whistleblowing, the burden of proving that the damaging consequences are not the result of whistleblowing shall lie with the employer.

An illogical part of this article is that the **definition of the term "damaging action" already includes connection to whistleblowing**. Article 2 defines the damaging action as "any action or failure to act in connection with whistleblowing, which threatens or violates rights of a whistleblower or any person entitled to protection as a whistleblower, or which puts that person at a disadvantage". Thus, while Article 29 seems likely that there is a connection between whistleblowing and a damaging action, or that attempts have been made to prove that there is no such connection, Article 2 stipulates that in cases when there is no such connection, there is no "damaging action" either! Linguistically speaking, a whistleblower or any person seeking protection before the court, has to "make probable" that "the action taken against them is in connection with whistleblowing"; however, the defendant has to prove that "the action taken against whistleblowers and related to whistleblowing, was in fact not caused by whistleblowing". This logical confusion can only be resolved by judges turning a blind eye and interpreting the definition of "damaging action" within the meaning of Article 29, and not Article 2, as an action which objectively harms a whistleblower or another person who enjoys protection, where the "connection" or causality will remain to be proven.

Principle of Investigation

Article 30

Principle of Investigation

In proceedings for judicial relief in connection with whistleblowing, the court may establish the facts even when these are not disputed by the parties, and may also independently investigate facts not presented by either party in the proceedings, if the court deems this to be important for the outcome of the proceedings.

This provision has not been established solely for the benefit of whistleblowers, although the report from the public debate states that this was the exact intent. **The court is equally bound to investigate the facts that are important for the outcome of the proceedings and that can help the defendant** avoid liability for retaliation they performed. For example, a violation of certain regulations happened in July 2015, and a whistleblower revealed it in December 2016. The whistleblower's lawsuit claims that they became aware of this event one month ago, when they gained access to the document. However, if during the proceedings whistleblower's statements or any other source suggest that the whistleblower was aware of all essential elements of the event back in August 2015, the court will be obliged to investigate this issue until the end and establish the truth, even if the defendant fails to request so. The legality of whistleblower's action and the right to protection will depend on whether the whistleblower acted within a specific subjective deadline or not.

Ruling in the absence of defendant

Article 31

Absence of Defendant

In case a duly summoned defendant fails to appear at the main hearing, the court may hold the hearing in the absence of the defendant, and may also rule on the basis of the facts established at the hearing.

Comment:

It is not clear what was the intention of the legislator with this provision. In fact, it has already been stipulated that the proceedings on the lawsuits filed by whistleblowers apply the provisions of the Civil Procedure Code applicable to labour disputes. This chapter also includes Article 440, Para 2, with an almost identical text as the Article 31 of the LPW. The only difference is that, according to the LPW, the court may hold a hearing without the presence of the defendant (but is not obliged to), while, according to the Civil Procedure Code, the court is obliged to do so ("the court shall hold a hearing"). Since the difference has not been explained, a logical assumption is that the legislator wanted to authorise the court to use its discretion to decide if a hearing needs to be held without the defendant who was duly summoned. Otherwise, this standard would not be necessary because of Article 440, Para 2 of the LPW would apply. Another possible explanation would be to interpret this situation as a random discrepancy and that the word may in fact implies both the authority and the obligation of the court to hold a hearing without a duly summoned defendant.

It is interesting to note that the parliamentary hearing also addressed the proposed amendments (deputy Olgica Batić), according to which the lawsuit would be deemed withdrawn if a whistleblower or other prosecutor failed to show up at the trial for two consecutive times, after being duly summoned, and do not justify their absence. The government has not accepted this amendment "because the decision of the Law is aligned with the Civil Procedure Code. It can be expected that the prosecutor, whistleblower, or a person who enjoys protection as a whistleblower, has an interest to solve the civil proceedings quickly, efficiently and without undue delay. In addition, the plaintiff is guaranteed a series of rights by the Civil Procedure Code (to justify their absence, restore the status quo ante, etc.), and for this reason the solution proposed by the amendment is unacceptable". The assessments that the prosecutor has no motive to stall the procedure are questionable. Interim measures may put the plaintiff at a favourable position, so the defendant is the one who considers as not guilty the person whose interest is to complete the process as soon as possible, and a whistleblower whose arguments are weaker can have the opposite motive.

Interim Relief

Article 32

Interim Relief and Jurisdiction

The court hearing the case pertaining to relief in connection with whistleblowing or a case referred to in Article 27 hereof may institute interim relief pursuant to legislation governing enforcement and security.

A motion to institute interim relief may be made before the initiation of proceedings for judicial relief in connection with whistleblowing, in the course of such proceedings, or until such time as the court ruling has been enforced.

During the course of the proceedings, the court may also institute interim relief ex officio.

Comment:

> Interim measures are determined on the basis of the Law on Enforcement and Security. We would like to note that, after the adoption of the Law on the Protection of Whistleblowers, a new Law on the procedure for enforcement and security was passed in late 2015, so it is possible that some of the solutions that the legislators had in mind when drafting this law differed from the standards that apply today.
>
> Although proposing an interim relief before court proceedings is a solution that also exists in the Law on Enforcement and Security, it is not clear why it was provided in the LPW. It is not clear why a whistleblower would not file a lawsuit along with a proposal for the interim relief. Both in cases of filing a lawsuit **and in cases of submitting a proposal for an interim relief, a whistleblower must "make probable" that they suffered negative consequences due to whistleblowing, and that a "damaging action" took place.**

Article 33

Interim Relief Prior to Initiation of Court Proceedings

The court with jurisdiction to hear lawsuits for relief in connection with whistleblowing shall be competent to rule on a motion to institute interim relief prior to the initiation of court proceedings.

When instituting interim relief referred to in paragraph 1 of this Article, the court shall also set a deadline by which a lawsuit must be lodged with the competent court, taking into account the deadlines for lodging lawsuits set under specific legislation.

Article 34

Motion to Grant Interim Relief

A motion to grant interim relief may petition the court to defer the entry of an enactment into legal force, prohibit the performance of a damaging action, and remedy the consequences of a damaging action.

The court shall rule upon any motion to institute temporary relief within eight days from the day the motion is filed.

Comment:

> The rules would certainly be more clear, and perhaps more conclusive, had it been specified that the court may order the "employer" or any defendant to take action on behalf of a whistleblower, if such action was within their powers and abilities. There are both similarities and differences between "eliminating the consequences caused by a damaging action", which may still be required, and the introduction of an opportunity to issue an order to the defendant. Eliminating harmful consequences and eliminating damaging action (which consists in failure to act) are two different things. If the Law was amended in this way, it would undoubtedly be possible to order the employee to issue a decision on allowing vacation days, to begin assigning tasks to an employee who was previously ignored, to solve the case of a party (if the whistleblower is a person not employed by the "employer", but a user of the services of that body), etc. However, the amendment that aimed to complement the standard in this way was not accepted "because it is unclear what constitutes an interim relief that would order the employer to take action on behalf of whistleblowers and associated persons".

Article 35

Appeal against Order Granting Interim Relief

A separate appeal shall not be permitted against a ruling granting interim relief.

MONITORING THE IMPLEMENTATION OF THE LAW

Article 36

Monitoring the Implementation of the Law

The Labor Inspection shall be in charge of monitoring the implementation of the Law, or Administrative Inspection, in accordance with the law governing their authorities.

This provision is unacceptably ambiguous. **The jurisdiction between the two aforementioned authorities is not clearly divided**, nor is it clearly stipulated that both of these inspections are responsible for the control of the implementation of all provisions of the Law. In order for the control to be effective, one state administration body should be in charge of monitoring the implementation of the Law, and other authorities that maintain or gain some control powers should be listed as well. This could be the Ministry of Justice, which normally governs the Law drafting process, in charge of by-laws and in partial control of the implementation of the Law, based on the decisions from the strategic anti-corruption laws. In any case, other ministries would continue to carry out activities within their jurisdiction: Ministry of Labor in connection with the implementation of labour regulations, Ministry of Health, Ministry of Trade, and others in connection with the provision of certain services to customers, and some forms of business cooperation, etc.

Neither of the two aforementioned control bodies has received new powers – it was only mentioned that they perform control in accordance with their existing powers. On that basis, the labour inspectorate deals with control in connection with labour relations, administrative inspection controls if the authorities that fall under the supervision of the body made all the required acts, and the like. However, **none of the control bodies has received the authorization to take care of the issues in "unassigned" sectors – the actions of businesses and other legal entities in relation to shareholders and business associates.** Because these sectors are not part of the public sector, administrative inspection does not control their work, but because these are not labour relations, labour inspection has no control either. Finally, another unassigned issue is the control of the implementation of the Law provisions related to dealing with "information" – **none of these inspections is responsible for monitoring the actions of "competent authorities" after they receive information from whistleblowers.**

POSSIBLE PENALTIES

Penal provisions do not stipulate offences. This is good from the standpoint of legal technique, as all offences should be covered by one provision, the Criminal Code. However, the proposal of the LPW was not accompanied by the proposal for amending Criminal Code, which is a big omission, because **some very harmful acts are currently not stipulated neither as criminal offence, nor misdemeanour offence**. What is even worse is that this omission has not been rectified before the beginning of implementation of the Law, or even in the years that followed, although there were opportunities to do so.

Article 37 stipulates fines for employers – legal persons, entrepreneurs, and responsible persons within these bodies. Article 37 stipulates the violations in cases of employer's failure to adopt a general act on internal whistleblowing, or failure to display such act in a visible place that is accessible to every employee. Article 38 contains all other violations:

- failure of the employer to protect whistleblowers from damaging action, to take measures for its suspension, and actions for the elimination of damaging action (Article 14, paragraph 2);
- failure of the employer to submit written notice of rights under this Law to all employees (Article 14, paragraph 4);
- failure of the employer to designate a person authorised to receive information and conduct proceedings in connection with whistleblowing (Article 14, paragraph 5);
- failure of the employer to act on the information within the prescribed period (Article 15, paragraph 2);
- failure of the employer to notify the whistleblower on the outcome of the proceedings within the prescribed period (Article 15, paragraph 3);
- failure of the employer to provide information to whistleblowers, upon their request, on the progress and actions taken in the proceedings, to enable them to examine the case files, and to attend the procedural actions (Article 15, paragraph 4).

Offences are not stipulated for violation of the following provisions (some of them are partly included in some of the stipulated offences):

- Article 3 (preventing whistleblowing);
- Article 4 (performing damaging action);
- Article 10 (failure to protect personal data of whistleblowers);
- Article 11 (the abuse of whistleblowing);
- Article 14, Para 1 (failure of the employer to take measures to eliminate irregularities indicated by whistleblowers);
- Article 14, Para 3 (taking measures by the employer for revealing the identity of anonymous whistleblowers);
- Article 16, Para 3 and 4 (expanding the general act with provisions that are not in accordance with the LPW and the Rulebook, or the provisions that reduce the rights of whistleblowers in relation to their legal rights);
- Article 18, Para 3 (failure of the competent authority to act within 15 days of receiving "information");
- Article 18, Para 5 (failure of the authority who received the information to implement the protection measures);
- Article 18, Para 6 (failure of the authority to seek consent for disclosure of the identity of whistleblowers);
- Article 18, Para 7 and 8 (failure of the competent authority to provide whistleblowers with information on the progress and actions taken in the proceedings, to allow them access to case files, to allow them access to procedural actions, or to inform them of the outcome of the proceedings);
- Article 19, Para 2 (failure of whistleblowers to respect the presumption of innocence of the accused, the right to protection of personal data, as well as the obligation not to jeopardise the conduct of the proceedings) – these forms of violations of the Law can be prosecuted under other legislation;
- Article 20 (acting against the Law on Data Secrecy) – these forms of violations of the Law can be prosecuted under other legislation;
- Article 21, Para 1 (putting whistleblowers at a disadvantage);
- Article 21, Para 2 (the adoption of a general act which deprives whistleblowers of their rights, infringes their rights, or puts them at a disadvantage).

THE BEGINNING OF LAW IMPLEMENTATION

Chapter VI

TRANSITIONAL AND FINAL PROVISIONS

Article 39

Deadline for Adoption of Bylaws

The enactment referred to in Article 17 and Article 25, paragraph 3 of this Law shall be adopted within three months of the entry into force hereof.

Employers shall be required to adopt the general enactment referred to in Article 16, paragraph 1 hereof within one year of the entry into force hereof.

Article 40

Entry into Force

This Law shall enter into force on the eighth day from the date of its publication in the Official Gazette of the Republic of Serbia, and shall enter into effect six months from the date of its entry into force.

“Monitoring the implementation” of the Law on Protection of Whistleblowers

As regards the implementation of the Law on the Protection of Whistleblowers, the only state authority that publishes reports is the Ministry of Justice, based on the obligation from the revised Action Plan for Chapter 23. The last report published by the Ministry refers to the 2015-2020 period.[5] Previously, there was a practice of issuing annual reports.

This report shows detailed statistics on the work of certain types of courts, which indicate that the number of resolved cases in 2020 was lower than in previous years (128 compared to 160), with a decline noted in all the categories except in the Supreme Court of Cassation (revision proceedings). It is the consequence of reduced inflow (117 compared to 152 in the previous year). The report’s assessments of the “overall quality “of court decisions are unclear. It is estimated that the quality in 2020 was 93.75%, although it can be seen from the overview that out of 25 considered appeals, 17 judgments were upheld, one was modified, and 7 were abolished. These data are important in the context of the fact that specialised training on the application of the Law on Protection of Whistleblowers was presented as a requirement for judges to even act in these cases; the question of the quality of these trainings, or the meaningfulness of such a legal provision, can therefore be reasonably raised, especially because 2020 was the sixth year of applying the Law.

When it comes to internal whistleblowing, the report of the Ministry of Justice contained only data on the application of the Law in the ministries, although a large number of other authorities, as well as economic entities, have statutory obligations in that regard. The number of recorded cases is still very low and declining compared to previous years (25, compared to 40 in 2019). All last year’s cases involved only two ministries – the Ministry of Defence and the Ministry of Interior.

It is a direct consequence of inadequately assigned supervision of the implementation of this Law. Two inspectorates (Administrative Inspectorate and the Labor Inspectorate) are authorised to perform it, but they are not clearly divided and do not cover all areas. The Administrative Inspectorate supervised the implementation of this Law in only four cases in 2020, while the Labour Inspectorate initiated 16 procedures as a result of 4,158 controls (relating to the application of various acts) conducted in 2020.

Although problems with the monitoring of internal whistleblowing were significant due to inadequate supervision, they were far greater in terms of external whistleblowing. In its report, the Ministry of Justice stated that “...given the fact that there is no statutory obligation for ministries to keep records of external whistleblowing,[6] they have different recording practices”, but it did not do anything to change the situation as the authorised proponent of the Law.

Transparency Serbia has on numerous occasions made proposals to solve this problem, both when the Law was in passing,[7] and during its implementation.[8]

5 https://www.mpravde.gov.rs/files/Izve%C5%A1taj%20o%20primeni%20Zakona%20o%20za%C5%A1titi%20uzbunjiva%C4%8Da%20(2015-2020).pdf

6 Ибид., p. 29.

7 https://bit.ly/3E8SgmT

8 https://bit.ly/2Zn8QjW

Did the protection of the whistleblowers advance reporting of corruption?

Reporting of corruption as an objective of the legislature

One of the main objectives of the Law on Protection of the Whistleblowers 2014 was reporting corruption. The word corruption is mentioned over 50 times in the explanation of the proposed law.[9]

This in part refers to the fact that the legislation was predicted by the National Strategy for the Fight against Corruption in the period from 2013 to 2018 (Official Gazette of the Republic of Serbia number 57/13), as well as the accompanying Action Plan ("Official Gazette of RS", number 79/13), international conventions ratified by Serbia and recommendations from GRECO.

As such, "the explanation of the problem that the proposition of the law has to solve" begins with the words "Persons who report suspicion of corruption or other unlawful behaviour... are not provided with adequate, sufficient or complete form of social protection". When it comes to expected effects of the application of the Law at the forefront is: "this legal frame provides the necessities for achieving the objective of support and encouragement for reporting suspicion of corruption or other unlawful behaviour as a way of protecting the public interest. It should contribute to the encouragement of potential whistleblowers and establish a mechanism for uncovering illegalities and irregularities."

Statistics of criminal prosecution

Passing of the legislation occurred over eight years ago. As it is mentioned in previous chapters, Serbia did not establish the system for gathering and tracking even basic information which are in connection to whistleblowing nor the ones concerning actions taken in response to whistleblowers reports of corruption. This is the reason why today it is still unknown to which extent are proclaimed objectives fulfilled. Data on the number of reported cases of corruption (no matter who reported them)[10] indicates that in the first year of applying the legislation the number of criminal reports has stayed on the similar level as before. A drastic increase occurred in 2018, though it was unnaturally instigated, while waiting for the new special departments for suppression of corruption within higher public prosecutor's offices to start operating. Hence the flour special departments of higher public prosecutor's office in 2018 had even 7,367 criminal reports[11] for criminal behaviour from their jurisdiction, while just next year that number was cut in half (3,903).[12] In 2020 it came to further reduction (2,936),[13] and in 2021 the number stabilised at 3,035[14] reports. The data cannot be fully comparable with the data from 2012-2017 because of the changes in Criminal Code and jurisdiction. It appears to be that those changes and, perhaps, a wide application of plea agreements, resulted in the increase in the number of criminal reports (almost 50%) that is easily noticeable from 2018 in comparison to the years before.

9 http://www.parlament.gov.rs/upload/archive/files/lat/pdf/predlozi_zakona/3140-14.pdf

10 https://preugovor.org/Infografici/1512/Statistika-gonjenja-korupcije-20122017.shtml

11 https://mpravde.gov.rs/files/Statistika%20koruptivnih%20krivi%C4%8Dnih%20dela%20-%20Posebna%20odeljenja%20za%20suzbijanje%20koprupcije%202018.pdf

12 https://mpravde.gov.rs/files/Statistika%20koruptivnih%20krivi%C4%8Dnih%20dela%20-%20Posebna%20odeljenja%20za%20suzbijanje%20koprupcije%202019.pdf

13 https://mpravde.gov.rs/files/Statistika%20koruptivnih%20krivi%C4%8Dnih%20dela%20-%20Posebna%20odeljenja%20korupcija%20RJT%20i%20VKS%202020.pdf

14 https://mpravde.gov.rs/

An effort to determine effects

Transparency Serbia attempted to deduce to which extent whistleblowing has assisted in reporting of corruption in another way. Since in Serbia majority of the forms of corruption have been criminalised, we have reached out to the public prosecutors office as a sole authority prosecuting these criminal offences. At the end of 2022, TS has sent a sequence of requests for access to information. Through these requests we have also reminded the prosecutors office that the submission of criminal charges could be viewed as one form of external whistleblowing in the context of the Law on Protection of the Whistleblowers. It is expected that the prosecutors office would already be familiar with the information, given that whistleblowers, as it is already noted, are entitled to some rights which are not guaranteed to everyone submitting a criminal charges.

The following has been requested:

1. Information and copies of all the documents form which is apparent how many criminal reports have been submitted by an external whistleblower, according to Article 18. Para 1 of the Law on Protection of the Whistleblowers (Official Gazette of the Republic of Serbia number 128/2014) to the public prosecutors office in the period from 5 July 2015 to the date of the submission of this request; and

2. Information and copies of all the documents form which is apparent how many notices concerning the outcome of the prosecutions of criminal reports from the first item of this request has the public prosecutors office… according to Article 18. Para 1 of the Law on Protection of the Whistleblowers (Official Gazette of the Republic of Serbia number 128/2014), delivered to the whistleblowers in the period from 5 July 2015 to the date of the submission of this request.

Those who did not reply

Institutions who have not given any answer to our request:

- Prosecutors Office for Organized Crime;
- Higher Public Prosecutors Office in Belgrade – Special Department for Suppression of Corruption;
- Higher Public Prosecutors Office in Niš – Special Department for Suppression of Corruption;
- Higher Public Prosecutors Office in Belgrade (for the period 2015-2018);
- Higher Public Prosecutors Office in Niš (for the period 2015-2018);
- Higher Public Prosecutors Office in Kraljevo (for the period 2015-2018);
- Higher Public Prosecutors Office in Leskovac;
- Higher Public Prosecutors Office in Prokuplje;
- Higher Public Prosecutors Office in Smederevo;
- Higher Public Prosecutors Office in Subotica.

What is apparent from the replies

In the first place, we want to express our gratitude to all the public prosecutors who have found the time to reply to our request and in that made possible, to us as well as the public, to get familiar with the application of the Law on Protection of the Whistleblowers and with authorities which are responsible for criminal prosecution.

The Higher Public Prosecutors Office in Kraljevo – Special Department for Suppression of Corruption was the first to request an explanation of our request. The Prosecution Office was in need of this explanation saying: "Taking into account that our records do not contain the information from which it could be determined if the criminal report has been submitted by a natural person in relation to working engagement, hiring process, using the service of state or some other body, business cooperation and the ownership rights over the company." This is already an eloquent answer to the question of the extent of possibility to track the fulfilment of the obligations stated in the Law on Protection of the Whistleblowers. Furthermore, they asked of us to state: "Weather there is a requirement for data concerning criminal reports in which the person submitting the report legitimises himself- as the whistleblower or is it enough for the person to have his properties stated in Act 2, item 2 of the Law on the Protection of the Whistleblowers".

After we made clear that we request both, we received the reply, in which the Special Department for Suppression of Corruption, with the beginning on 1 March 2018, received only two criminal reports from "persons who called on the status of a whistleblower". When it comes to those who did not refer to this status even though they might fulfill all the requirements to be recognised as a whistleblower, Higher Public Prosecutors Office in Kraljevo did not submit the data, referring to the fact that it concerns a big amount of information, implying it would require an insight in every individual case. Lastly, when it comes to the outcome of the process, we received no information "as it may uncover the identity of the whistleblower" that the Prosecutor's Office is required to protect.

The Special Department of Higher Public Prosecutors Office in Novi Sad provided us with considerably more information. Since this department has been founded they have received ten criminal reports "which commenced external whistleblowing in terms of Article 18 of the Law on Protection of the Whistleblowers. We have received an anonymised abstract of those reports, as well as anonymised parts of criminal charges. In some cases these reports are not in relation to corruptive criminal behaviour and for that reason have been forwarded to other Prosecutors Offices. Corruption reports are submitted anonymously and in most cases by employees (in most cases those who work in the public sector). In some cases Higher Public Prosecutors Office in Novi Sad has informed us that they were unable to clearly identify whether those submitting the reports were really whistleblowers, in other words if they were employees of the companies or bodies against which the reports were submitted or if they had a different relationship.

Reports were submitted against managers of the public companies, chiefs of municipal administrations and other municipal managers, manager of one public institution and in few reports as perpetrators were named members of public and private sector alike for whom it is claimed to have organised corruptive affairs at the expense of the budget.

Conduct in the period from 2015 to 2018

If the replies from Public Prosecutors Offices are to be believed, whistleblowing is a completely unmarked territory, not only in cases of corruption but in general. We have been informed by the Public Prosecutors Offices in Pančevo, Jagodina, Čačak, Kruševac, Novi Pazar, Požarevac, Sombor, Užice, Valjevo, Vranje and Zrenjanin that from 5 June 2015 to November of 2022. "There have been no submissions of the reports concerning external whistleblowing" (which is the most common formulation). Formulation from Jagodina is different in replay "Higher Public Prosecutors Office in Jagodina did not act according to the reports submitted by the whistleblowers, that is, the subject were not recorded in record books labelled "U" and "I" concerning conduct according to the Law on Protection of the Whistleblowers.

The Higher Public Prosecutors Office in Novi Sad has informed us that since the establishment of the Special Department for Suppression of Corruption (on 1 March 2018) there have been no submissions of reports by whistleblowers.

The Higher Public Prosecutors Office in Kragujevac has received two criminal reports during 2016, and one in 2017 and all of them had been forwarded to Public Prosecutors Offices.

We received a reply from the Higher Public Prosecutors Office in Negotin that entails that the Higher Public Prosecutors Office received one report from a whistleblower which has been forwarded to the Public Prosecutors Office. This Higher Public Prosecutors Office has informed us that according to their knowledge the Public Prosecutors Office in that city has conducted another report of the same nature that concerned breaking the policy of public procurement.

The Higher Public Prosecutors Office in Pirot has received one report from a whistleblower in 2015. During that process, as we have been informed, three plea agreements have been signed and against two parties the process is nearing resolution.

In Sremska Mitrovica two whistleblowing reports have been submitted that have been forwarded to the Higher Public Prosecutors Office in Novi Sad as it falls under their authority.

What conclusion can be drawn from the received replies

From the received replies we can draw a conclusion that the number of criminal reports that are being submitted by the whistleblowers, whether their concerning corruption or some other crimes, is very low. However, that conclusion would not be true in its entirety. Keeping in mind the broadness of the definition of the whistleblower, it is practically impossible that over the period of seven years none of the Higher Public Prosecutors Offices have been submitted any. On the contrary, this is a clear indication of an absence of a system in prosecutors offices obligated to track the fulfillment of duty according to the Law on Protection of the Whistleblowers, nor any kept records of the submissions by which the exact number of submissions concerning “external whistleblowing” could be determined. These proceedings should not only be under the authority of the public prosecutors offices, but rather belong to the authority of the Ministry of Justice itself, which during the drafting of the Law did not take into account the need for tracking and perception of the effects of the changes.

On the other hand, it is apparent that many public prosecutors offices keep in mind the obligation in terms of external whistleblowing only in cases where the person filing the report identifies as a whistleblower or if their legal representatives do so. This rises hope that with right instructions that would come from the top of the prosecution hierarchy or by forcing changes of bylaws according to new judicial regulations, this field could be better organised.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

342.726-057.1:343.353(497.11)
3.083(497.11)
3.077:343.352(497.11)
316.334.3(497.11)

NENADIĆ, Nemanja, 1972-

Whistleblowing in Serbia and EU Directive / [author Nemanja Nenadić]. -
Belgrade : Transparency Serbia, 2023 (Belgrade : Unagraf). - 74 str. ; 30 cm

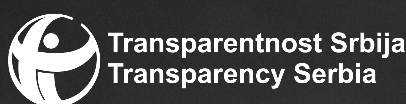
Nasl. izvornika: Узбуњивање у Србији и ЕУ директива. - Podaci o autoru
preuzeti iz kolofona. - Tiraž 100. - Napomene i bibliografske reference uz tekst.

ISBN 978-86-84711-56-6

а) Узбуњивачи -- Заштита -- Србија б) Политичко понашање -- Србија
в) Јавна управа -- Корупција -- Србија

COBISS.SR-ID 110648585

ISBN-978-86-84711-56-6



Transparency Serbia is non-partisan, non-governmental and non-for profit voluntary organization established with the aim of curbing corruption in Serbia.

Transparency Serbia's main goal is to increase transparency in the work of state organs as a way to prevent abuse of public authority for private purposes, through preventive activity - raising public awareness about the dangers and damage that corruption does to society, fostering reforms and proposing concrete recommendations.

Transparency Serbia is national chapter and representative of Transparency International in Republic of Serbia.

www.transparentnost.org.rs

TransparencySer

Transparentnost.Srbija