Ukraine Nazar Chernyavsky

**1. Is the use of software without sufficient licenses a criminal or administrative offence? What are the preconditions and consequences of such an offence?**

Depending on the amount of pecuniary damages caused by the use of software without appropriate licensing, such usage may be classified as criminal or administrative offence.

Article 176 of the Criminal Code of Ukraine stipulates that illegal reproduction, distribution, and other infringements of copyright resulting in considerable damage (from about EUR 560 up to about EUR 5,600 in UAH equivalent) shall be classified as a criminal offence. This criminal offence is punishable with a fine (up to EUR 590 in UAH equivalent) or correc-tive labour for up to two years, or imprisonment for the same term.

If the same actions are committed repeatedly or upon prior conspiracy by a group of per-sons, or if these action result in extensive damage (from about EUR 5,600 to up to about EUR 28,000 in UAH equivalent), it is punishable with a fine (ranging from about EUR 590 up to about EUR 1,180 in UAH currency equivalent), or corrective labour for up to two years, or imprisonment from two to five years.

If the above illegal acts are committed by an official through abuse of office or committed by an organized group of persons leading to particularly extensive damage (more than UAH equivalent of about EUR 28,000), it is punishable with a fine (ranging from about EUR 1,180 to about EUR 1,790 in UAH equivalent) or imprisonment from three to six years, to-gether with a possible additional ban on occupying certain positions or conducting certain activities.

The form of guilt is only direct intent. Moreover, IP rights infringement cases belong to pri-vate prosecution cases. This means that a criminal case can only be initiated based on an application from a legal entity or individual that has information about the criminal offense or by a victim.

The above criminal liability is central in cases of copyright infringement. However, depend-ing on the peculiarities of the individual crime, it can be combined with other crimes (cumu-lative crime). By way of example, Article 203-1 of the Criminal Code of Ukraine provides for liability for illicit disc circulation for laser reading systems, matrices, equipment and raw materials for their production. The punishment for the latter actions is a fine.

Where pecuniary damage is less than UAH equivalent of about EUR 560, then such of-fences with respect to use of the software without license will be classified as an adminis-trative offense. The punishment imposed is a fine (from EUR 6 to EUR 590 in UAH equiva-lent) with confiscation and destruction of the infringing goods, equipment, and materials used for any illegal production. The form of guilt for these infringements can only be direct intent.

Finally, as in the case with criminal law, the Code of Ukraine on Administrative Offences contains provisions on the illegal production, export, and import of discs for laser reading systems, and on illegal export and import of equipment and raw materials for their produc-tion (Article 164-13). The punishment for these actions is a fine.

Because discs are no longer the main means of committing piracy, both criminal and ad-ministrative liability for illegal production, export and import of discs for laser reading sys-tems and on illegal export and import of equipment and raw materials for their production are less relevant for business.

## 2. Does a statutory right to conduct software audits exist under your jurisdiction's (copyright) law?

Ukrainian statutory law does not explicitly entitle the rights holder to conduct software au-dits.

However, Article 52 of the Law of Ukraine "On Copyright and Neighboring Rights" ("Copy-right Law") allows for the application of the following means of protection of rights:

- (i) Take part in inspection of production facilities, warehouses, and techno-logical processes and commercial operations related to the manufacture of the copies of the copyrighted works suspected of infringing or threatening to infringe the rights. The rights holder can be engaged in inspection in accordance with the procedure approved by the Cabinet of Ministers of Ukraine. According to Item 20 of the Regulation on Intellectual Property State Inspector of the Intellectual Property Service of Ukraine approved by Resolution No. 674 of the Cabinet of Ministers of Ukraine dated 17 May 2002 (as amended) ("Inspection Procedure"), the Intellectual Property State Inspector may decide to engage the rights holder upon the request of the latter. Notably, Inspection procedure permits the rights holder to engage consultants and other experts for inspections.
- (ii) Demand information about third parties engaged in production and distri-bution of counterfeit copies of copyrighted works from the infringer. This right is not straightforward. In order to exercise it, the rights holder must apply for an appropriate order from the court.

In addition, in order to protect copyright, Article 53 of the Copyright Law grants the courts the authority to apply the following temporary measures to preserve evidence of an in-fringement:

- (i) Inspection of those premises where acts associated with the infringement of copy-right are believed to be occurring;
- (ii) Arrest and seizure of documents that can serve as evidence of the infringement or possibility to infringe copyright.

These measures can be applied at the rights holder's request before filing a lawsuit, or if the infringer does not provide access to the premises or information. Such requests must be considered within two days after filing with the court. The temporary measure order is subject to immediate enforcement by state enforcement agencies with participation of the rights holder.

Notably, before applying temporary measures, the court is entitled to require the posting of a bond by the rights holder. The bond value should not be less than the UAH equivalent of about EUR 60 and must be more than the amount of the claimed damages.

It also worth mentioning that the same measures can generally be applied according to the Commercial Procedural Code of Ukraine and the Civil Procedural Code of Ukraine without regard to the provisions of the Copyright Law.

In practice, requesting temporary measures by the rights holders is extremely rare due to difficulties with substantiation of the need for taking such measures before the court (irre-spective of whether provisions of the Copyright Law are applied or the rights holder relies on the provisions of the respective Procedural Code only).

## 3. Are contractual software audit clauses subject to restrictions under contracts law?

Based on the freedom of contracts principle stipulated by the Civil Code of Ukraine, we believe that software audit clauses are valid if individually negotiated by the parties to a li-cense agreement. The rights, remedies, and procedures stipulated in Articles 52 and 53 of the Copyright Law generally support this position.

However, it is important to note whether said audit clauses comply with general principles and requirements of the Ukrainian contract law. In particular, to avoid any potential claims of abuse

of IP rights and, thus, increasing the risks of audit clause invalidation, we believe that it is important to balance the audit procedure within such clauses (e.g., prior audit no-tice, limitation of the audit to premises, documents and information that directly relate to the possible infringement).

At present, we are not aware of any jurisprudence declaring such audit clauses to be valid or void.

## 4. Are there any co-determination rights of the workers' council with respect to software audits?

No.

## 5. What are the data protection limitations to software audits?

Personal data processing during the course of software audits is subject to limitations pre-scribed by the Law of Ukraine "On Personal Data Protection" ("PDP Law"). The PDP Law defines personal data as information or data relating to an individual, who is identified or identifiable. Notably, while the PDP Law does not contain any express provisions on its territorial effect, it can be argued that it also applies to processing of personal data that relates to Ukrainian citizens or residents regardless of where the data operator is established, server is located, or personal data are processed.

It seems that the parties would need to comply with the above requirements when a par-ticular natural person is specifically and intentionally identified for some legitimate rea-son(s). An IP address per se is usually not sufficient to qualify as personal data.

Pursuant to Article 6 (5) of the PDP Law, personal data may only be processed for expressly described and justifiable purposes. Licensor and licensee should comply with this requirement irrespective of legitimate reason of personal data processing.

The PDP Law requires that the data subject must consent, not only to processing its per-sonal data for a specific purpose, but also to the (i) scope (categories) of personal data subject to processing; (ii) information on how personal data will be used; (iii) information about dissemination of personal data; and (iv) information about access of third parties to personal data.

However, as is the case in other jurisdictions, it may be impractical for the controllers to rely on employee consent as for example, this consent may be revoked by the employees at any time.

It worth mentioning that obtaining consent is not the only legitimate reason of personal data processing. In addition and as an alternative to obtaining consent, the following legitimate reasons may be the most relevant for software audits:

- (i) Protection of legal interests of a data controller or a third party to which personal data is transferred. The PDP Law also stipulates that the need for protection of the discussed legal interests should outweigh the need for personal data protection. The latter should be discussed and decided on a case-by-case basis.
- (ii) Processing is necessary for the establishment, exercise or defense of legal claims. This legitimate reason is applicable only to processing of sensitive personal data (Article 7 of the PDP Law) and cross-border transfer of personal data to jurisdictions which do not ensure an adequate level of protection of personal data (Article 29 of the PDP Law).

There is also a general legal requirement to notify the data subject in relation to personal data collection on the day of collection (if collected from individual) or within 30 business days after such collection (in all other cases). The PDP Law sets specific requirements to the content of the notification (e.g., purpose of personal data collection, third parties to whom its personal data can be transferred).

In addition, the data subject must be notified within 10 business days about each modifica-tion, deletion, or the destruction of its personal data. In practice, many Ukrainian data con-trollers choose to take a risk-based approach in relation to this requirement, on the basis that as of now, the likelihood of enforcement for non-compliance with this PDP Law re-quirement is relatively low.

Finally, once so-called extreme risk data (e.g., any pre-trial procedures applied to the per-son, any investigative procedures against the person, location and travel routes) are going to be collected and processed, it is important to notify the Ukrainian DPA about such pro-cessing. The Ukrainian DPA should be notified within 30 days of commencing any extreme risk data processing.