# Some aspects of the provision of information security in the engagement of international criminal jurisdiction organs

## Деякі аспекти забезпечення інформаційної безпеки у діяльності органів міжнародної кримінальної юрисдикції

Tetyana Syroid, Lina Fomina

*Key words:*

*information and communication technologies, international criminal litigation, means of provision of security, provision of security.*

*Ключові слова:*

*забезпечення безпеки, інформаційно-комунікаційні технології, заходи забезпечення безпеки, міжнародне кримінальне судочинство.*

In today's digital age there is a wide-spread application of the achievements of science and technology, particularly information and communication technologies (hereinafter – ICT) and media that permeate all aspects of life and open up great opportunities. The organs of international criminal jurisdictions (International Criminal Court, International Criminal Tribunal for the former Yugoslavia, Special Court for Sierra Leone, Special Tribunal for Lebanon, Extraordinary Chambers in the Courts of Cambodia, etc.) in their activity also use ICT, that greatly facilitate the process of law enforcement, in particular, promote effective systematization of information contained in electronic media, make public aware of the proceedings, accelerate the speed of data transfer etc. However, the use of ICT can have negative consequences in the field of information security, such as: leak of data (confidential data), amending the information sources (of evidence, texts of the documents, etc.) or disabling the entire e-court system. Such illegal actions are detrimental to each individual member of the international criminal justice (those, who give effect to the implementation of the challenges of international criminal justice and trial participants' rights, victims, witnesses and perpetrators of crime) as well as to the court information security in general. In view of the above, information security is an integral part of effective and independent administration of justice and enforcement of rights of the members of international criminal justice.

**The purpose** of the article is to analyze the statutes, procedural and other internal acts of international criminal jurisdiction organs concerning the consolidation of the provisions on information security.

The objectives to achieve the purpose above-mentioned are as follows: study the provisions of the statutes, procedural and other internal acts of international criminal jurisdiction organs concerning the consolidation of the provisions governing information security; highlight information security measures; make appropriate conclusions.

**Basic material research.** There is a great importance of using information and communication technologies (hereinafter – ICT) in many spheres of social life, and the system of justice is not an exception. Thus, ICT are widely applied in administering justice, particularly, to improve information processing, transmission and publishing, enforcement of trial participants' rights, etc. It is important to stress that when administering justice the key aspect is to provide data security, which is hold by the court, prosecutor, attorney etc., as it can contain information on location area of certain persons, materials concerning the state of the proceeding, records of witnesses and crime victims, etc.

In view of the fact that a great part of information concerning the administration of justice retains in electronic systems of the international organs of criminal justice, there is a threat of its modification, damaging or using by the third parties for their own benefit. With this in mind, acts (statutes, rules of procedure and evidence, regulations etc.) of such organs contain the provisions on regulation of data security issues.

The provisions of procedural acts of the international criminal organs (International Criminal Court (hereinafter – ICC), International Tribunal for the Former Yugoslavia (hereinafter – ICTY), Special Court for Sierra Leone (hereinafter – SCSL), Special Tribunal for Lebanon (hereinafter – STL), Extraordinary Chambers in the Courts of Cambodia (hereinafter – ECCC) prove the above-mentioned.

Thus, in accordance with the provisions of Regulations of the Court ICC the Court shall establish a reliable, secure, efficient electronic system which supports its daily judicial and operational management and its proceedings. The Registry shall be responsible for the implementation of the system described in sub-regulation 1, taking into account the specific requirements of the judicial activity of the Court, including the need to ensure authenticity, accuracy, confidentiality and preservation of judicial records and material. Documents, decisions and orders shall, whenever possible, be submitted in electronic version for registration by the Registry. The electronic version of filings shall be authoritative (Regulation 26 (1–3) Regulations of the Court ICC)[1].

The provisions for the establishment of electronic document management systems are also provided by the internal acts of ICTY and STL. Thus, the Practice Direction on the application of an electronic court management system (ICTY) states that this Practice Direction is issued in order to provide a framework for a reliable and secure electronic system to support the efficient management of court proceedings (art. 1). The Protocol for the Upload of Electronically Stored Information (STL) indicates that the Tribunal has adopted and implemented an electronic document management system (the Legal Workflow System – LWS) (p. 1).

According to the Regulations of the Court ICC the e-court system is an information system which manages and provides access to judicial records and material. In consultation with the relevant organs of the Court and participants, the Registrar shall establish and update a list of persons authorised in the proceedings to access, through the e-court system, judicial records and material (Regulation 10 (1–2) Regulation of the Registry ICC).

It is also important to emphasize that the Registry shall keep information relating to witnesses, victims who appear before the Court, persons at risk, as well as the dependants of all such persons, and accompanying support persons in a secure environment. A secure electronic database shall be maintained for any information relating to persons referred to in sub-regulation 1. This database can only be accessed by designated staff members of the Registry (Regulation 88 (1, 3) Regulations of the Registry ICC).

For the purposes of the Regulation 97 (Confidentiality of communications) the Registry shall maintain a secure electronic database for the storage and processing of information provided in applications from victims, any documentation or further information supplied by victims or their legal representatives, and any communications received from or in respect of such victims including communications or other information from or relating to specific victims that have been made available to the Registry by other organs of the Court (Regulation 98 (1) Regulations of the Registry ICC)[2].

There is a provision that the Registry shall respect and protect the confidentiality of non-public documents in the Practice Direction ICTY as well (art. 4(5)).

The importance of this issue for the appropriate security protection is supported by the Presidential Directive ICC/PRESD/G/2005/001 «Information Security Policy» (hereinafter – Directive), which sets out provisions on information security enforcement[3]. Thus, it is, particularly, stated that such policy addresses the protection of the confidentiality, integrity and availability of its information against threats including error, fraud, sabotage, terrorism, extortion, espionage, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental. The Court requires that information important to its functions is adequately safeguarded to protect the public and the Court's interests.

The Directive emphasizes that the President, Prosecutor and Registrar shall ensure the proper design, implementation and management of effective information security arrangements. Users of information must comply with the security provisions and restrictions placed on them by the Court.

---

[1] Regulations of the Court ICC ICC-BD/01-05-16 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsCourtEng.pdf.

[2] Regulations of the Registry ICC ICC-BD/03-03-13 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.

[3] Presidential Directive Information Security Policy ICC/PRESD/G/2005/001 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.

It is also stated that providing an appropriate level of information security requires a systematic and coordinated approach where the level of protection corresponds to the assessed level of risk. The protective measures to be taken to mitigate the perceived risks can be of a procedural, technical and physical nature. The selection of appropriate protective measures shall be based on a sound factual, financial, lawful and ethical basis. Most importantly, they must be based on an assessment of risk.

Information shall be classified, based on a formal classification system, to indicate the need, the priority and desired level of protection. Classification ensures that information is protected according to the degree of harm that could result from its unauthorized disclosure. Information wherein is defined as all types of information, regardless of its medium, that is produced, transmitted, and stored for and by the Court.

Classification of information in accordance with the levels of confidentiality is also provided by the Practice Direction "Classification and management of case-related information" ECCC/004/2009/Rev.2 (art. 3), Practice Direction on Filing of Documents before the Residual Special Court for Sierra Leone (art. 5), Practice Direction on filing of documents before the Special Tribunal for Lebanon (art. 6).

There is an important guarantee of information security fixed by the President Directive ICC "Information Security Policy" under which the Court shall actively promote amongst staff and officials awareness and knowledge of information security and the issued policies, procedures, standards and guidelines on information security. Staff and officials shall immediately report any suspected security incidents, suspected viruses, software malfunctions, faults, weaknesses or threats observed or suspected to the information and Information Systems of the Court. The Information Security Officer (ISO) has been delegated responsibility for the Court's information security process and shall coordinate and monitor the information security efforts in the Court. In addition, the ISO shall provide to the ICC and its organs advice on risks, opportunities and measures with regard to information.

In order to realize the objectives of this Presidential Directive, the Court will continuously monitor its Information Systems and register all usage and transfers of information, irrespective of the method or form of such transfer. Whenever there is a reasonable suspicion that there may have been a violation of any information security policies, procedures, standards or guidelines, the Court shall immediately investigate the matter and take such actions as are required to protect the confidentiality, integrity and availability of the information and restore the proper functioning of the Information Systems.[4]

The Administrative Instruction ICC/AI/2007/002 on "Information Security for Mobile Devices and Portable Storage Media" states that it relates to the sensitivity of the information on mobile devices (such as laptops) and portable storage media (such as CDs and USB sticks) in use by staff. The secure usage of mobile devices and portable storage media will mitigate the risk of information compromise and potential embarrassment for the Court through loss and theft. Thus, The Court gathers, stores, processes and disseminates information. Much of this information is sensitive in the sense that unauthorised disclosure or modification might compromise the Court, its reputation, cases, witnesses, staff, officials or other interlocutors. Such information must be protected in a consist manner[5].

The AI ICC/AI/2007/002 defines "Mobile Devices" as Laptops, Tablet PCs, Personal Digital Assistants, mobile telephones and all future portable mobile computing devices introduced in the ICC that can store, process and dispatch information and that are intended for usage inside and outside the ICC; "Portable Storage Media" – any carrier designed and used for solely storing and transporting (but not transmitting) information. The Court also determines "Users" as all staff members, Elected Officials of the ICC, Visiting Professionals and Interns/Clerks, Consultants, Contractors and other persons granted access to ICT Resources.

There is a specific guarantee of information security of the Court stated in AI ICC/AI/2007/002, according to which Mobile Devices used for processing, storing and dispatching information shall have measures in place that prevent the execution of Malicious Code, where the term "Malicious Code" means a piece of programming code that causes some unexpected and undesirable effect and which has the possibility to harm or abuse users, information or devices.

---

[4] Presidential Directive Information Security Policy ICC/PRESD/G/2005/001 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.

[5] Administrative Instruction Information security for mobile devices and portable storage media ICC/AI/2007/002. [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20for%20Mobile%20Devices%20and%20Portable%20Storage%20Media.PDF.

It is necessary to point out that by threats, concerning the safe and controlled storage, processing and dispatching of information on Mobile Devices, the Court recognizes: Execution of Malicious Code; Unauthorized Access to information; Unauthorized Communication. Thus, according to the AI ICC/AI/2007/002 Mobile Devices used for processing, storing or dispatching information classified as "ICC RESTRICTED" and above, shall have measures in place that prevent Unauthorized Access; Mobile Devices used for processing, storing and dispatching information classified as "ICC CONFIDENTIAL", shall have measures in place that prevent Unauthorized Communication; Mobile Devices used for processing, storing or dispatching information classified as "ICC SECRET" may be used stand-alone or in a network only if such network or network connection is under control of the Court. Privately owned Mobile Devices and Portable Storage shall only contain information classified as "ICC RESTRICTED or below".

The requirements for the physical protection of Portable Storage Media may be met by either adequate digital encryption of the Portable Storage Medium in its entirety or by digital encryption of the classified information on a per file basis.

Furthermore, AI ICC/AI/2007/002 states that Users shall sign for the receipt of Mobile Devices and tokens that are assigned to them. The ICT Service Desk shall administer the assigned Mobile Devices and tokens assigned to Users.

As provided by the AI ICC/AI/2007/002 the care and protection of Mobile Devices and Portable Storage Media is the responsibility of the individual User. Users shall not connect Mobile Devices other than Court provided Mobile Devices to the Court's network. Administrators of the ICT Section may connect Mobile Devices other than PDAs to the Court's network for testing, installation, maintenance and backup purposes.

Provision, which states that any key, token, username, password or other mechanism that gives access to the Mobile Device or the Portable Storage Media shall not be transported together with the Mobile Device or the Portable Storage Media to which it gives access, acts as the guarantee of provision of information security.

Upon detection of any shortcomings in the measures in place in respect of the Mobile Device or Portable Storage Media, Authorized Users shall: (a) Stop using the Mobile Device and / or Portable Storage Media; (b) Notify the ICTS Service Desk[6].

The issue of information security is declared in Administrative Instruction on "Information Security in Agreements with Third Parties" ICC/AI/2007/005 dated 19/06/2007 (hereinafter – AI ICC/AI/2007/005) [5]. Third Party is a party, outside the Court, which has a contractual agreement with the Court and has a contractual obligation to provide goods and/or services but is external to the Court. A Third Party can be an entity, an individual, or a group of individuals. Examples of Third Parties include but are not limited to: (a) Cleaning and other outsourced maintenance and support services; (b) External ICT maintenance and support services; (c) Experts, Trainers and Consultants.

The ICC uses the services of «Third Parties» for various tasks and on a constant basis. Information might be put at risk when accessed by Third Parties with a security regime that does not match the Court's security regime. Hence, formal arrangements involving Third Party access to the Court and the Court's information shall be established and incorporated in contracts, processes and infrastructure. This Administrative Instruction sets out the Court's practice for protecting the confidentiality of its information throughout its use of Third Parties.

The AI ICC/AI/2007/005 in question aims to: (a) Define the requirements to provide controlled and secure access for Third Parties to Court information; (b) Clarify tasks and responsibilities with regards to information security to staff that are involved in setting up and managing agreements with Third Parties; (c) To minimize the potential exposure from damages which may result from unauthorized use of the information by and/or due to Third Parties (sub-section 2.2).

The AI ICC/AI/2007/005 applies to Third Parties with access or potential access to the Court's classified information regardless of the form of such access. Contracts with Third Parties shall contain provisions on the following responsibilities and obligations of Third Parties: (a) Third Parties shall respect confidentiality with regards to the information of the Court; (b) Third Parties shall comply with the Court's formal information security policies,

[6] Administrative Instruction Information security for mobile devices and portable storage media ICC/AI/2007/002 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20for%20Mobile%20Devices%20and%20Portable%20Storage%20Media.PDF.

procedures and standards; (c) Third Parties shall be responsible for their staff and for any sub-contractor working for the Third Party; (d) Third Parties shall be responsible for the screening of their staff and any sub-contractor working for the Third Party and shall be able to provide evidence to the contents and outcome of such screening; (e) Third Parties shall maintain a list of individuals who are permitted to use the type of access and services as provided by the Court on the Third Party's behalf; (f) The obligation of a Third Party to comply with the legislation pertaining to the Court; (g) Third Parties shall respect the intellectual property right of information and software provided by and to the Court (sub-section 3.3).[7]

Moreover, AI ICC/AI/2007/005 prescribes that the Court Contract Owner shall make the Court's formal information security policies, procedures and standards available to the Third Party. Third Parties that are expected to have access to sensitive Court information on a regular basis shall be briefed by the Information Security Unit of the Registry's Security and Safety Section on the Court's formal information security policies, procedures and standards (sub-sections 4.1, 4.3).

**Conclusions.** Therefore, we came to the conclusion that proper access to information and information transfer definitely improves the efficiency of international judicial organs, gives equal opportunities for all the participants of legal proceedings. However, it is important to note that such technological advances as data-processing system and computer networks make users of these services subject to risk. The number of e-crimes is growing rapidly, besides, criminal associations use service forms of cybercrime market to commit crimes against the states, their institutions, individuals and juridical entities, and also to commit more cunning types of crime such as illicit trafficking in cultural property, child abuse and abusive child labour, wildlife trade, credit card identity fraud etc.

From this perspective, databases of the international organs of criminal jurisdiction are at stake, particularly the one of the International Criminal Court, which has crucial evidential information on commission of the most serious international crimes, orders of perpetrators of such crimes, information on crime victims etc. Such information can be employed criminally. To prevent these illegal actions International Criminal Court adopts relevant acts (administrative instructions, directives, information circulars, etc.) to ensure the security of the Court and trial participants. Such acts focus on provision of information security, they, in particular, categorize information in accordance with the level of risk; establish procedures for the use of mobile devices and portable storage media, data access procedure for the third parties and so on. All the above-mentioned acts supply and clarify procedural acts of the ICC, creating a legal basis for proper functioning of the Court and provision of information security.

## *Summary*

The article is devoted to the analysis of the provisions of statutes, procedural and other acts (administrative instructions, directives, information circulars, practice directions) of the international criminal jurisdiction organs (International Criminal Court, International Criminal Tribunal for the former Yugoslavia, Special Court for Sierra Leone, Special Tribunal for Lebanon and Extraordinary Chambers in the Courts of Cambodia) on the provision of information security; we have also considered the means of provision of security while using the information and communication technologies; finally, we have made relevant conclusions.

## *Анотація*

У статті проаналізовано положення статутів, процедурно-процесуальних та інших внутрішніх актів (адміністративні інструкції, накази, інформаційні циркуляри, практичні керівництва) органів міжнародної кримінальної юрисдикції (Міжнародного кримінального суду, Міжнародного трибуналу щодо колишньої Югославії, Спеціального суду щодо Сьєра-Леоне, Спеціального трибуналу щодо Лівану, Надзвичайних палат у судах Камбоджі) щодо забезпечення інформаційної безпеки; приділено увагу заходам забезпечення безпеки під час використання інформаційно-комунікаційних технологій, зроблено відповідні висновки.

[7] Administrative Instruction Information security in agreements with third parties ICC/AI/2007/005 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20In%20Agreements%20with%20Third%20Parties.PDF.

## *Literature:*


1. Regulations of the Court ICC ICC-BD/01-05-16 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsCourtEng.pdf.
2. Regulations of the Registry ICC ICC-BD/03-03-13 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.
3. Presidential Directive Information Security Policy ICC/PRESD/G/2005/001 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Documents/RegulationsRegistryEng.pdf.
4. Administrative Instruction Information security for mobile devices and portable storage media ICC/AI/2007/002 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20for%20Mobile%20Devices%20and%20Portable%20Storage%20Media.PDF.
5. Administrative Instruction Information security in agreements with third parties ICC/AI/2007/005 [Electronic resource]. – Access mode : https://www.icc-cpi.int/resource-library/Vademecum/Information%20Security%20In%20Agreements%20with%20Third%20Parties.PDF.



***Tetyana Syroid,***
*Ph.D. in Law, Professor, Professor of the Department of International and European law*
*V.N. Karazin Kharkiv National University*

***Lina Fomina,***
*lecturer of the department of International and European law*
*V.N. Karazin Kharkiv National University*