Architecture of the National Classification of Legal Regimes of Restricted Access Information

Dmitrii Lovtsov
Department of Information Law, Informatics and Mathematics
Russian State University of Justice
Russian Federation, Moscow
dal-1206@mail.ru

Dmitrii Makarenko
National Legal Service, LLC
Russian Federation, Moscow
d.g.makarenko@gmail.com

Andrei Fedichev
Legal Information Scientific Centre of
Ministry of Justice of the Russian Federation
Russian Federation, Moscow
andrey.fedichev@scli.ru

***Abstract*—Purpose of the paper: improving the scientific and methodical base of the theory of legal regimes of information resources. Method used: conceptual and logical modelling of the legal concept and productive facet-cum-hierarchical classification of pragmatic types and kinds of classified information. Results obtained: based on the principle of heterogeneity of the concept of information and classified information, the architecture (conceptual and logical organization) is justified and the conceptual and methodical base (principles-rules of classification, methods of coding of classification elements, classification groupings) is developed for creating an efficient national classification of legal regimes of restricted access information as a regulation subject to further standardization and inclusion in the list of Russian classifications contained in the Russian Classification of Information on Russian Classifications. The place and role of the national classification of legal regimes of restricted access information in the system of Russian classifications are shown.**

Keywords—privileged information; data; relational model; classified information; legal protection

The information concealment in the clandestine regime as secret (having a secrecy label - the secret regime) and confidential information is now the primary way of legal protection (safeguarding) for privileged information (having a tangible, moral and any other value due to its being unknown to third parties), e.g., scientific and technical information, financial, economic, production, structural information and know how, market, patent, license etc. information, from third parties' access.

The clandestine and secret varieties number over 50 in Russian law (taking into account international treaties). Their common feature is that the information protection in the clandestine regime envisages [1]: the person's/ entity's statutory right to introduce the restricted access regime; establishment and restriction of the scope of the holder's rights to protected information and his/her duties to protect the same and to disclose it at the requests of competent governmental agencies as well as liability for breach of established rights and duties.

However, the laws are mostly codifying the private and applied approach, whereby the clandestine (secret) means the information itself that should be protected from unauthorized access and use in order to prevent harm to interests of parties to legal relations. This leads to confusion of the notions of clandestine, including secret and privileged information (new data for a recipient), and to confusion of types of clandestines and secrets.

In the modern legal science, clandestine means a special legal regime of privileged information as a package of legal tools that describe a combination of interrelated prohibitions, permissions, enforcements, entitlements, incentives (privileges) and sanctions, i.e. the legal regime of concealment and/or legal protection of privileged information [2]. That is to say, the same data (information) having certain potential "novelty", i.e. the information value for a certain range of persons, may belong to different legal regimes without change in their information content, may be subject to clandestine (secret) of the appropriate type and kind. For example:

data on the essence of certain new industrial properties (inventions, pre-production prototypes, utility models) can be simultaneously subject to the state clandestine regime of the entity acting as the governmental R&D customer, to the business secret regime of a non-public organization (defense industry enterprises etc.) acting as R&D developer, and to official secret of a leading employee of the entity acting as R&D support customer;

individual's personal data may be simultaneously subject to the personal (private) clandestine regime, tax (office) clandestine and bank (professional) clandestine;

data on the private digital signature key may be subject to the personal clandestine regime, if the digital signature keys are generated independently, and also simultaneously to the personal clandestine regime and the office (professional) clandestine regime, if the keys are generated by the public (commercial) Certification Center (Key Certification Center) etc.

An array of correlating clandestine varieties (information and legal regimes) necessitates the substantiation of an intelligent system intended for legal protection of privileged information where a consistent classifier (from Latin classis meaning "category" and facere meaning "to do") of legal regimes for the sensitive information is the key component serving as the streamlined list of the information and legal regimes, each having the matching unique code. The classifier enables to identify functional relationships among the components, i.e. the regimes of the legal protection system for privileged information, and among the respective legal relations that arise, in order to discover and estimate the pragmatic features of the information security law sub-industry integrity [1]. The classifier shall also allow for unification of computer databases and streamlining of the computer-aided sharing of privileged information in federal and municipal information systems [3].

An array of legal regimes for the restricted access information in the classifier can be conventionally divided, according to the well-known [2] efficient relation model of the legal notion of clandestine (Table 1), into four classification groupings: public, private (personal, family, commercial), office and professional clandestine.

TABLE 1.

Relation model of the legal notion of "clandestine"			
Type of clandestine	**Legally significant clandestine types**		**Type of information legal relations (essence)**
	of public law nature	***of private law nature***	
Basic *(clandestine is the target)*	Public	Private	Absolute *(protection against encroachment)*
Derivative *(clandestine is duty)*	Office	Professional	Relative *(protection against breach)*

The basic and derivative clandestines as targets of information legal relations arising out of the authority and subordination, one of the parties to which is a public authority, i.e. public information legal relations, also have the public law nature. In particular, it is public and office clandestines.

However, the clandestines as targets of civil (private) information legal relations arising out of the independence of will, equality and proprietary independence of the parties, have the private law nature. In particular, it is personal and family clandestines, business, bank, insurance and testament clandestine (which are recognized by the law-maker as civil right items, in Articles 150, 139, 857, 946, and 1123, Russian Civil Code, respectively). The particular feature of these information and legal regimes is that the privileged content itself ("new" data), subject to the legal regime of a certain clandestine, is a special sort of intangible benefit and, as such, can also be the target of information legal relations (besides the regime) having the protective (rather than regulatory) nature [4].

These four basic components (see Table 1) contain inter-related subsets of clandestine (secret) varieties, the main of which being, in particular:

1) state clandestine of governmental authorities, including: military, foreign policy, economic, intelligence, counter-intelligence, anti-terrorist, geological etc. secrets; industrial, operational search etc. clandestines;

2) private clandestine of individuals or legal entities (private life or business clandestine), including such clandestine varieties as:

- private life clandestine, which comprises two inter-related clandestines:

personal clandestine of an individual, citizen, national etc., including: clandestine of religion, political views and voting, diaries and personal records, personal life (including love affairs, in particular, when related to adultery; vicious social past and defamatory business and amicable connections); physical (hidden physical defects) and mental state (sexual preferences, bad habits, inclinations, choices, congenital, hereditary and acquired vices, sometimes bordering on nervous and mental abnormalities), etc.

family clandestine of relatives, including: clandestines of adoption, intimate relations, communication and creative work, joint family life etc.

-commercial clandestine of an individual or legal entity as the business entity, including: securities and invention clandestine; production secrets (know how), corporation, trading process (insider), craft etc. secrets

3) office clandestine protected by a public servant, including: tax, audit, voting, state registration, fingerprint, social service recipient, security effort clandestines (with respect to the judge and other legal proceeding participants, officers of law enforcement and supervisory authorities), clandestine of investigation, legal proceedings (conference of judges, conference of jury, of legal proceeding participants), of enforcement proceedings, of personal data of military men of the Interior Ministry's internal forces, etc.;

4) professional clandestine protected by a professional business entity: clandestine of confession, pawnshop, communication (correspondence - mail, telegraph, computer and other messages; telephone calls, etc.), journalist (editorial) clandestine, clandestine of legal efforts (of legal counsel, insurance, testament, of notarial efforts, mediation procedure), bank clandestine (of bank accounts, deposits and transactions; of the credit history), medical clandestine (doctor's, donor's), etc.

The legal protection regime is not determined for a lot of individual restricted access data (e.g., data in connection with the procurement of goods, work, services to meet federal and municipal needs; data and proposals contained in the submitted applications for participation in the tender, when an indebted enterprise is sold; or enterprise price proposals before the start of tender or before granting access to the applications submitted as e-documents for participation in tenders; data that became known to individuals during operating investigations; data pertaining to the mediation procedure etc.), mentioned in federal law, which necessitates the creation of a classifier under development.

Besides, many clandestines are comprehensive by nature, being the clandestines of lines of business, including different types and varieties of clandestines and secrets, and production clandestines are the tool for implementing the basic clandestines, so the liability for their compromising (unauthorized access, disclosure) may be established for all offences. For instance, breach of professional clandestine via unauthorized access (Article 241, Russian Criminal Code) to computer information, which resulted in getting acquainted with the information that constitutes state clandestine (Article 283.1, Russian Criminal Code), gives rise to criminal liability as the perfect set of crimes (under both articles of the Russian Criminal Code).

The relation model of the legal notion of clandestine (see Table 1) is the blueprint for substantiation of a uniform, consistent system of one-for-one connection between the types of possible information legal offences and those of relevant penalties. As well as for development of the appropriate inter-related set of information and legal regimes (ILR) that perform special protective and defense functions of heterogeneous privileged information and enabling, in the aggregate, to implement the principle of balanced interests of a personality, the community and the State, while improving and developing the information law in order to support their multi-faceted information security [5].

With the use of this relation model for building up the classifier, the classification of information and legal regimes into independent ("parallel") classification groupings (facets) and their subsets (classes, categories) is carried out according to the well-substantiated principles, based on the established features of discrepancy or similarity of information and legal regimes, using the combined facet and hierarchical method. The set of classification groupings shapes a hierarchic quasi-arborescent structure as a branching free chart where groupings serve as nodes. A large information capacity, tradition nature and regularity of application, the possibility of creating the meaningful mnemonic codes for classification items (Table 2), and a certain flexibility of the structure hinging upon the possibility of including new information and legal regimes into one of the four classification groupings, are the main advantages of such method.

TABLE 2.

Structure of the classifier of legal regimes for restricted access information	
Code	**Clandestine types and kinds**
100.000.000	**TARGETS OF CLANDESTINE (basic)**
101.000.000	**STATE CLANDESTINE**
101.001.000	Military secrets
101.002.000	Foreign Policy and Economy Secrets
101.003.000	Industrial clandestine
101.004.000	Intelligence, counter-intelligence, operational search and anti-terrorist secrets
101.004.001	*Operational investigation clandestine*
101.005.000	Transport security secrets
101.006.000	Geological secrets
102.000.000	**PRIVATE CLANDESTINE**
102.001.000	**Private life clandestine**
102.001.100	**Personal clandestine**
102.001.101	*Religion clandestine*
102.001.102	*Clandestine of diaries and personal records*
102.001.103	*Clandestine of political views and voting*
102.001.104	*Physical and mental state clandestine*
02.001.200	**Family clandestine**
102.001.201	*Family life clandestine*
102.001.202	*Adoption clandestine*
102.002.000	**Business clandestine**
102.002.001	*Securities clandestine*
102.002.002	*Invention clandestine*
102.002.003	*Trade secrets*
102.002.004	*Craft secrets*
102.002.005	*Production secrets (know how)*
102.002.006	*Corporate secrets*
200.000.000	**CLANDESTINE - DUTIES (derivative)**
201.000.000	**OFFICE CLANDESTINE**
201.001.000	Tax clandestine
201.002.000	Audit clandestine
201.003.000	Voting clandestine
201.004.000	State registration clandestine
201.005.000	Fingerprint clandestine
201.006.000	Social service recipient's clandestine
201.007.000	Security effort clandestine
201.008.000	Investigative clandestine
201.009.000	**Legal proceeding clandestine**
201.009.001	*Clandestine of judge meetings*
201.009.002	*Clandestine of jury meetings*
201.009.003	*Clandestine of legal proceeding participants*
201.009.000	Clandestine of enforcement proceedings
201.010.000	Clandestine of personal data of military personnel of the Interior Ministry's internal forces
202.000.000	**PROFESSIONAL CLANDESTINE**
202.001.000	Confession clandestine
202.002.000	Pawnshop clandestine
202.003.000	Connection clandestine
202.004.000	Journalist (editorial) clandestine
202.005.000	**Clandestine of legal efforts**
202.005.001	*Legal advisor's clandestine*
202.005.002	*Insurance clandestine*
202.005.003	*Clandestine of notary actions*
202.005.004	*Testament clandestine*
202.005.005	*Mediation clandestine*
202.006.000	**Bank clandestine**
202.006.001	*Bank deposit clandestine*
202.006.002	*Credit history clandestine*
202.007.000	**Medical clandestine**
202.007.001	*Doctor's clandestine*
202.007.002	*Donor's clandestine*

The following basic principles-rules [6-8] are used for building up the classifier:

- pragmatism (practical relevance and immediate use), i.e. only classification groupings and signs required for addressing some particular objectives of legal protection (safeguarding) of privileged information should be included into the classifier;

- non-overlapping of classification groupings, i.e. the composition of signs in one grouping must not be repeated in others;

- guaranteed legal protection, i.e. inclusion of the information and legal regime into the subset (class, category) of the regimes described by the set of legal tools that guarantee legal protection (safeguarding) of the privileged information;

- compatibility, i.e. conformity to the requirements of the Unified System for Classification and Encoding of Technical, Economical and Social (Including Social and Legal) Information of the Russian Federation (USCE of TESI) etc.

The combined parallel and sequent method is used for encoding the classifier elements, i.e. assigning a code to the classification grouping (facet) or the classification item (information and legal regime): the classification signs inside a facet are encoded independently from each other by certain categories or a group of categories of code designation. In addition, all information and legal regimes in the classifier are described, for referential purposes, by availability of regulations and laws (R&L), indicating liability for their violation [9, 10] (see the Appendix).

A scientifically-substantiated classifier of legal regimes of restricted access information, as the basic component of a sound system for legal protection of privileged information will be able to influence the structure of electronic data of legal proceedings in all Russian courts and also the improvement of legal methods used in drafting regulations in this field. Their application in legal proceedings takes the precise regulatory determination of the single meaning of the laws that govern the similar social relations, so that to ensure their sustainability and uniform understanding of the law and judicial practice. Thus, the systematic and stable legal terminology is formed in constitutional, civil, administrative, criminal, and arbitration proceedings [11].

The Unified Classifier of Legal Regimes of Restricted Access Information may become an important tool for securing the terminological unity of legal proceedings and also an efficient tool for integration of electronic information resources of judicial and law enforcement authorities and may align the system for classification and encoding privileged information with global and Russian classifiers and standards.

Thus, based on the efficient use of the well-known relation model of the legal notion of clandestine, which enables to develop the functionally sufficient and consistent set of protective information and legal regimes, as well as the well-substantiated classification principles and rules, the conceptual and methodical basis of creating an efficient national classifier of legal regimes for restricted access information was elaborated, as a regulation subject to further standardization and inclusion in to the list of Russian classifiers, which is contained in the Russian Classifier of Information on Russian Classifiers.

REFERENCES

[1] D. Lovtsov, “Systematology of legal regulation of information relations in information sphere”: article thesis, Moscow: RGUP, 2016, 316 pp.

[2] D. Lovtsov, “Conceptual and logical modeling of the legal notion of clandestine”, Informational Law, 2009, issue No. 2, pp. 12-14.

[3] D. Lovtsov, A. Fedichev, “Place and role of legal informatics in information and legal knowledge”, Legal Informatics, 2017, issue No. 1, pp. 5-12.

[4] V. Kopylov, Informational Law. Moscow: Moscow State Legal University, 2005, 510 pp.

[5] D. Lovtsov, Informational Theory of Ergasystems: Thesaurus. Moscow: Science, 2005, 248 pp.

[6] V. Omelchenko, General Classification Theory, Part 1: Basics of Reality Cognition Systematology. Preface by D. Lovtsov. Moscow: Librocom, 2008, 436 pp.

[7] V. Omelchenko, General Classification Theory, Part 2: Theoretical and Array Grounds. Preface by D. Lovtsov. Moscow: Librocom, 2010, 296 pp.

[8] D. Lovtsov, Bases of Linguistic and Informational Support of Automated Control Systems, in 2 books, Book 2: Information Base. Moscow: V.A. named after Peter the Great, 1990, 147 pp.

[9] D. Lovtsov, A. Kovalenko, “Development of the national classifier for legal regimes of restricted access information”, Proceedings of the VI Russian Scientific and Practical Conference Modern Continued Education and Innovative Development (April 20, 2016), FIRO FGAU, Serpukhov: IIF MOU, 2016, pp. 706-709.

[10] Fedichev A., Artamoshkin S. The Systematisation of Types of Relationships and Responsibility in Acquiring Access to Information. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2014, No 2(3), pp. 51-59. DOI: 10.21681/2311-3456-2014-2-51-59.

[11] D. Lovtsov, V. Niesov, “Topical issues of creating and developing the information space in the Russian judicial system”, Informational Law, 2013, issue No. 5, pp. 13-18.