THE USE MADE OF NOMINATIVE OR PERSONAL DATA ON THE INTERNET AND THEIR TRANSFER FOR TRADING PURPOSES

Ph. D. Associate Professor **Daniela Gărăiman**

Abstract: *The paper analysis the use made of nominative or personal data on the Internet and their transfer for trading purposes. The term spam does define electronically messages of trading nature, which and user could receive, in his own e-mail box, in massive quantities and with no request made for them. The cookies are local data files, passive, encrypted and personalized, which are inserted by the sites on a computer, through the surfing browser, at the moment when they would be accessed by the surfer. In recent years, the use of e-mail inside of companies has hugely amplified, this mean of communication becoming unavoidable. More and more companies place at the disposal of their employees computers with access to Internet and one or many e-mail addresses.*

Key words: *spam, cookies, internet transfer.*

1. The spamming. Definition and functioning

The term *spam* does define electronically messages of trading nature, which and user could receive, in his own e-mail box, in massive quantities and with no request made for them. They belong to the category of *unrequested messages* of whatever nature (economical, political, cultural, religious, etc.) received, with no request, in massive quantities, by an user, in his own e-mail box. In this category might be included the following types of messages:

- concatenated letters;
- pyramidal schemes;
- marketing made upon several levels;
- schemes with instructions about a quick welfare to be obtained through the network;
- offers made for pornographically sites;
- offers made for pirate software's; etc.

The sending of unrequested messages might be realized as a result of previously collecting e-mail addresses. This collection might be realized in various ways:

- due to the user's wilful registration on a certain website;
- from a list of e-mail addresses provided to the spammer by third sides;
- through automatically collection of e-mail addresses from the public space of Internet (webs, forums, etc.).

For the forwarder, the use of spam does not involve high financial investments or a lot of time to spend on it as he makes no effort in order to verify the addresses that he has collected by fraud. Generally, to launch such messages are employed automatically programs for collecting the addresses and accounts from free servers to release the messages.

There are three main modalities possibly used for sending spams:

1. to use your own e-mail servers;
2. to use servers provided by suppliers specialized in the domain of e-mail;
3. To use the e-mail servers of other Internet users, which have no protection system in this regard, or are not sufficiently protected.

Among the collecting methods, the most controversial in regard to the protection of personal data is the automatically collection of e-mail addresses from the public space of Internet. In the case of the other two methods, it is known that the user has wilfully agreed to provide his own address for registration. On the other hand, though the forwarder makes almost no investments for spamming, it might become expensive for their recipient to cope with such e-mails. So, the recipient might waste some time to erase them, either as simple messages from his e-mail box, or by following the method indicated by the message itself in order to erase his own e-mail address from the forwarder's list. The problems might not end yet, since the previously indicated erasing method

might not be efficient, therefore unable to produce the expected consequences. Further more, the recipient should have to assume the cost itself of receiving that many messages.

Methods of annihilation. In order to strive against spamming, various methods were defined. The main two methods are designated by the systems: *opt-in regime* and *opt-out regime*. Each of these two might be strengthened through complementary actions taken. The *opt-in regime* consists in forbidding the sending of advertising messages without the previous accept given by the recipients.

This formula may be realized in two ways: either the supplier should send the messages, but stating that the recipient would have the opportunity to refuse receiving unrequested advertising messages through a simple electronically message, or then the supplier should send to the recipient a previous expressed request of his agreement to receive advertising communications from him. When this condition would be satisfied, the supplier still should give an exact return address, and should accurately identify himself towards the recipient. Insofar, this second option ought to be preferred, since it could be able to cut down the advertising not requested messages' cost transfer towards their recipients.

The opt-out regime does authorize the sending of the unrequested electronically messages, in the absence of the recipients' refusal. Obviously favoured by the direct marketing companies, this type of regime requires an active role taken by the users, which might be realized by two possible ways: either under the form of an universal inclusion list, wherefrom each user should have the opportunity of refusing one or the other among the categories of electronically unrequested messages (political, cultural, trading ones, etc.), or by the opportunity, offered to the users, of withdrawing their own e-mail addresses from the forwarders' distribution lists.

Complementarily to these 2 types of regimes, in order to assure their respective efficiencies, some accessory actions might be taken. So, *an opt-in regime* might be accompanied by the obligation of correctly identifying himself for the forwarder. A penalty might be stipulated for the possible forgeries existing in the messages' headings. The *opt-out regime* might be accompanied by measures able to impose to the forwarders a previous taxonomizing of their commercial messages that should allow to the access' suppliers and to their users to select among the received messages.

Legislative evolutions. The European Directive nr. 58/2002, on the processing of personal data and on privacy's protection in the domain of electronically communications, does precise that automatically calling systems, bearing no human intervention, applied to fax and e-mail addresses, might be used for trading purposes, but only due to a previous agreement from the recipient. Similar stipulations are included to the Directive 31/2000, on the electronically trading, art. 7.

In the U.S.A. no federal law has been issued on spamming, though the first project about this matter was presented in 1997. The most recent project, entitled: *Controlling the Assault of Non-Solicited Pornography and Marketing Acts*, presented in March 2003, suggests that non-requested trading messages should be labelled as such (not necessarily through a standard method), that they should include instructions for opt-out and that they should include the forwarder's physical address. This project does forbid the use of deceitful address lines and of the forged headers for such messages[1].

Yet, in the U.S.A. most of the states have adopted an anti-spam legislation, which averagely imposes the obligation of providing *opt-out* instructions and/or the inclusion of a valid responding address[2]. In Romania, the Law nr. 365/2002 on electronically trading has forbidden commercial communications through e-mail[3], exception made of the case when the recipient had previously expressed his consent to receiving such communications (art. 6, par (1) of the Law).

---

[1] http://www.spamlaws.com.

[2] Only the states of Florida, Kentucky and Oregon are deprived of such legislations

[3] According to the law, by commercial communication should be understood: "any form of communication destined to promote, directly or indirectly, the products, services, image, name or designation, firm or emblem pertaining to a trader or to a member of a liberal profession; do not constitute, by themselves, commercial communications, the following:
- information allowing direct access to the activity of an individual or moral person, especially in the cases of domains' designations or e-mail addresses;

The consent communicated through a message sent by e-mail would be enforced as valid if the following conditions should be simultaneously fulfilled:

a) the message is forwarded from the e-mail box where the forwarder (future recipient) wishes to receive the commercial communications;

b) the subject of the message is formed by the concatenation of the text: "I accept commercial communications from ...", written in capital letters, and the name, or the denomination, of the person on behalf of which the commercial communications should be transmitted[4].

2. The cookies. Use, creation, access

The cookies are local data files, passive, encrypted and personalized, which are inserted by the sites on a computer, through the surfing browser, at the moment when they would be accessed by the surfer. Two types of cookies do exist:

- *the session cookies*, which have no lapsing date and which are automatically erased at the moment when the client shuts down his browser;

- *the persistent cookies*, which are preserved upon the visitor's disk and which are not erased by the browser's shutting down.

Problems might rise about the cookies, related to:

the modalities of their creation;

- the type of information they could contain;

- the way of accessing them;

how they might be destroyed;

- their legal status.

Cookie files are created by the browser through which the user is surfing on Internet, at the command given by a site that was accessed by the user. The sites which command the creation of such files are the sites which do interact with the surfer "in real time". These sites may be servers profiled on trading, on e-mail delivery, on news and other information, etc.

The cookie files contain information with personal value for the user which accesses the respective site (name, first name, address, e-mail address, type and frequency of accessed information, etc.) and/or information about the system through which the respective site is accessed (name of the computer, name of the domain to which the computer pertains, I. P. number, type of employed browser, name of the user who opened the surfing session, etc.). The cookies' information might be accessed by:

- the user of the computer on which the cookie was created;

- the site which ordered the cookie's creation;

- any site which should command the access to the former site. Keeping into account the fact that the information from a cookie file is encrypted, suiting an algorithm, and with a key, both known only by the site who had ordered the cookie's creation, we are able to say that only the site having created the cookie has, practically, access to the cookie's information.

The legal status of cookie files. The legal status' problem of cookie files has two matters involved:

- the legal status of their creation; and

- the legal status of the use made of their contained information.

Suiting the modalities through which cookies are created, there are 3 methods for obtaining information:

1. Through a form to fill in, the user is asked about which personal data would he agree to be recorded. By inscribing the information into the form's cases and by its validation, the user gives his accept about the recording of these data. So, keeping into account the usual practice of Internet

---

- communications made by a third side, independent from the concerned person, especially when made in perfect gratuity, related to an individual or moral person's products, services, image, name or trade marks".

[4] Government's Decision nr. 1308/2002 on the approval of the Methodological Application Norms for the Law nr. 365/2002 on electronical trading; the former's art. 7 par. (3)

surfing, he accepts willingly the creation of the cookie file. The user is also warned about what data he would be obliged to fill in, in order to have access to the respective site;

2. The information about the system which calls for the respective site is automatically read by it. Next the accessed site will, have the option to expressed ask for consent about recording it or not to ask for it;

3. The accessed site records information about the type of data accessed by the user, the search frequency related to these data, their downloading (total, partial, or no use made of them), with or without the warning of the user about gathering such information.

The purpose of recording data through cookie files might be:

a) to create databases of its own, to be distributed upon the computers of users, in order to ease the access to the respective site;

b) to make use of the respective information in order to improve the site's contents of information and for the purpose of advertising;

c) to make use of the respective information in order to exchange databases with other co-operating sites.

The sites which command the creation of cookie files may combine one or many methods of obtaining information, combining them next with one or many methods of using it. If the user should give his accept both about the category of information he would like to provide to the site and about how the site might make use of it, then, legally speaking, we would be entitled to say that the user's personal rights and liberties are, indeed, respected.

But, whenever data are picked up or used of without the consent of the user, following the situation's general and particular contexts, as well as the usual practice applied in such cases, the problem would rise of determining if any of the user's rights or personal liberties were (or not) infringed. The international organisms of our domain are hostile to these procedures, because they are formed without the user knowing it, and they are considered as dishonest gathering of information.

International organisms do recommend that users should be, explicitly and previously, informed about these programs' contents and duration, about how they might be refused and about the consequences of the refusal on the opportunity to visit the respective site[5].

Modalities of destroying cookie files. Starting from the premise that the user is the absolute master of his computer's resources, so, implicitly, of how its external memory should be allotted, the fact is obvious that, if the user should detain some minimal knowledge on computing systems and operational systems, then he would be able, at any moment, to erase the cookie files, definitively or temporarily, partially or totally. At the moment when the cookie files of a site are erased, the following consequences might appear:

- the access might continue to be granted, because the data from the respective files were also previously recorded into a database owned by the accessed site, but then, the cookie files destroyed by the user should be automatically re-created;

- the access might be forbidden, until the moment when the user should fill in another registration form; this situation occurs when the site has neglected to create a database of its own too, able to save data from the cookies;

- the access might continue to be granted, because the site should keep on creating cookie files, without asking for the user's consent.

Any browser allowing the surfing on the Internet is equipped to permit the realization, in regard to the modality of creating cookie files, of the chosen one among the following settings:

- not to create cookie files, at the request of the sites, without previously asking the user about that;

- to pose the question to the user, about their request of creating cookie files;

- to create automatically cookie files, at the sites' request, without asking the user about that.

---

[5] L. Bochurberg, *Internet et commerce électronique*, Ed. Dalloz, Paris, 2001, p. 98.

3. The persons' protection in regard to the processing of personal data and of their free circulation

Restriction brought to the processing of personal data. In view of the perspective of harmonizing the domain's legislations at the European level and following the line of the Directive issued by the European Union's Parliament and Council on the persons' protection in regard to the processing of personal data, and to their free circulation, the Romanian parliament has approved, on November, 21-st 2001, the Law nr. 677, with the purpose of guaranteeing and protecting the individuals' fundamental rights and liberties, especially the right to intimacy, to familial and private life, in regard to the processing of personal data[6].

Any processing of personal data should be performed only if the concerned person has previously given her consent in regard to this processing, expressed and unequivocally. The following restrictions were imposed:

- it is forbidden to process personal data pertaining to the person's origin, either racial or ethnical, to her political, religious, philosophical and other opinions, to her affiliation to a syndicate, as well as to her status of health or to her sex life (art. 7 par. (1)).;

- the processing of a person's numerical code or of other personal data bearing a generally applicable function of identifying her should be performed only if: a) the concerned person has given expressed her consent or b) the processing is expressed stated by a legal stipulation (art. 8);

- the processing of personal data pertaining to the perpetration of infractions by the concerned person, to penal convictions, security measures or administrative or disciplinary sanctions applied to her, may be performed only by or under the control of public authorities, within the limits of the powers granted to these letters by the law and under the conditions established by the special laws which govern these matters (art. 10).

The consent of the concerned person is not required, in the following cases:

- when processing is necessary in view of executing a contract or pre-contract of which the concerned person is a side, or in view of taking some actions, before concluding a contract, or pre-contract, at the concerned person's request;

- when processing is necessary in view of protecting the life, physical integrity or health of the concerned person, or of whatever other person might be menaced;

- when processing is necessary in view of the fulfilling of some legal obligation assumed by the operator;

- when processing is necessary in order to accomplish some measures of public interest or pertaining to exerting the prerogatives of public authority that the operator was invested with or the one of the third side to which data are revealed;

- when processing is required by the realization of a legitimate interest of the operator or of the third side to which data are revealed, under the condition that this interest should not prejudice, the concerned person's interest or her fundamental rights or liberties;

- when processing does concern data that could be obtained from documents that, suiting the law, are accessible to the public;

---

[6] By personal data (art. 3) should be understood any information concerning an identified or identifiable individual person, that is to say someone who might be particularly identified directly or indirectly, by the reference made to an identification number or to one or many items that should be specific for the individual's identity. The items' nature might be: physical, physiological, psychical, economical, cultural or social. By processing of personal data should be understood any particular operation or set of operations performed upon someone's personal data, through automatical means or other, such as:

- collecting, - extraction;
- recording; - consultation;
- organizing; - making use of them;
- stockage; - juxtaposing or combining them;
- adapting; - blockage; - destruction;
- modifying; - erasure;
- revealing them to third sides through transmission dissemination or in any other way.

- when processing is made for exclusively statistical purposes, or for historical or scientifically research, and data should remain anonymous, for all the processing's duration.

Rights enforced. The law also institutes the rights of a person, pertaining to the processing of her personal data. So, in the case when the personal data would be obtained directly from the concerned person, the operator should be obliged to provide to the former the following information:

a) the identity of the operator and, if necessary, the identity of its representative;

b) the purpose for which the processing of data is done;

c) supplemental information like:

- the data's recipients or at least the category of to be recipients;

- if the supplying of all categories of data is or not compulsory, and what would be the consequences of the refusal of supplying them;

- the existence, for the concerned person, of the rights stipulated by the present law, especially of the rights of access, of intervention upon her own personal data and the right of opposition, as well as the conditions required for exerting these rights.

In the cases when data should not be obtained directly from the concerned person, the operator would be obliged, at the moment of collecting the data, or, the latest, till the moment of their first revealing to third sides, if such a revealing should be intended, to provide to the concerned person, at least, the following information, unless the concerned person is aware of it already:

a) the identity of the operator, and, if necessary, the one of its representative;

b) the purpose for which data processing should be done;

c) supplemental information, like:

- what categories of data are at stake;
- the data's recipients or these categories;
- the existence of the rights stipulated by the present law for the concerned person, especially of the rights of access, of intervention upon her own data and the opposition right, as well as the circumstances when they could be exerted[7] (art. 12).

The access right to the data[8], the intervention right upon her own data[9], as well as the opposition right[10] are rights of which any person does benefit.

In view of securing data confidentiality , the law stipulates (in its Chapter VIII – *Contraventions and sanctions)* that the following deeds do represent contraventions and would be penalized through:

- the operator's omission to notify;
- the ill-intentioned notifying;
- the illegal processing of personal data;
- the ignoring of the confidentiality obligation;
- the operator's refusal to provide information to the survey authority.

---

[7] The following exceptions are allowed:

- the data processing would be performed exclusively for journalistic, literary or artistic purposes;
- the data processing would be performed for statistical purposes or for scientifical or historical research, and it should provide indications about the employed information sources;
- in any other situations where supplying such information would be impossible or would involve a too large effort in comparison with the legitimate interest that might be empeached;
- in the situations where the law expressedly states the data's recording or revealing.

[8] Any concerned person has the right to obtain from the operator, on her demand and for free, once a year, the confirmation of the fact that the data which concern her are or not processed by this latter (art. 13).

[9] Any concerned person has the right to obtain from the operator, on her demand and for free, the data's: actualizing, rectifying, blocking or erasure, especially for the mistaken or incomplete data, the data lacking conformity could also be transformed into anonymous ones (art. 14).

[10] The concerned person has, at whatever moment, due to legitimate and justified reasons related to her private situation, the right to oppose herself to the processing of data which concern her, exception is made in the case when contrary legal stipulations do exist (art. 15).

4. Nominative data, used of by the employee

In recent years, the use of e-mail inside of companies has hugely amplified, this mean of communication becoming unavoidable. More and more companies place at the disposal of their employees computers with access to Internet and one or many e-mail addresses.

But with this fact, the problem arrived of how to control the messages leaving from the respective e-mail boxes, or entering them. Since the employers have raised the control claim over these e-mail boxes, the employees came to invoke privacy's protection and its aspects. In order to eliminate these quarrels, a first solution should be that the employee should sign a form through which his employer brings to the former's knowledge the functioning statute of the e-mail system, as well as the monitoring modalities used over it.

The Appeal Court of the State of California has also decided towards this sense in the case Bourke vs. Nissan Motor Corp. During a sample session regarding the functioning modalities of e-mail exchanges between a dealer and the Nissan company, e-mails exchanged between the dealer's employees and the companies were chosen at random. Due to this sample session, the claimant, employed by Nissan, got fired. The reason of this fact was that a private e-mail was presented through this random selection, which contained personal data concerning the sex life which did not fit with the regulations of internal functioning of the e-mail system, which had been accepted by the claimant through his signature, when he was hired.

In the case when the employee did not sign for acknowledging a regulation for the e-mail's functioning and monitoring system, there are a lot of reasons standing for the employer's legal possibility of accessing electronically information forwarded or received by the employees through their professional e-mail box. Firstly the employers might argue about an exaggerated use made by their employees of the e-mail, for their own private purpose. This fact might constitute a problem, because the intense use made of e-mail could indeed become expensive, financially, for the employer.

On the other hand, the unreasonable use of e-mails might prejudice the company's public image[11]. Secondly, the employers may prove that, for an employee, the e-mail access is a necessity, insofar this latter is involved in the conclusion of contracts or establishing some relationships for the company[12]. Thirdly, it might be necessary to access the employee's e-mail box in order to preserve it from informatics viruses.

Even in the case when the employer should "promise" to the employee the confidentiality respect of the latter's e-mails, the arguments presented beyond would still enable legally the employer to access the information electronically receipted or forwarded by the subordinates through their professional e-mail addresses. The Federal Court of Pennsylvania has decided in this sense, on the case Smyth vs. Pillsbury.

The defendant "had promised" to the claimant the respect, during his employment contract, of the e-mails' confidentiality. Yet, the defendant was monitoring the e-mail server's activity as well for sending as for receiving e-mails, for the alleged reason of protecting itself from damages brought to its trading reputation.

Due to the impact of Internet and computing techniques upon all the society's activity domains, more and more employees demand to the employer the access to an e-mail box. This fact effectively leads to supplemental financial expenses for the employers. So, most of them, do elaborate real monitoring strategies in regard to professional emails, in order to:

- diminish expenses, by a rational use of this resource;
- avoid the deterioration of their trading image;
- prevent the employee's infractions, possibly perpetrated through electronically means.

Yet, these strategies of e-mails' monitoring ought to respect, as it should be possible, this correspondence's secret.

[11] For example, if the employee would transmit pornographical images.

[12] For example, in the case of the employee's absence, it might be necessary to access the messages which would require urgent responses from the company.

If the employee should wish for a safer confidentiality of his own private e-mail correspondence, he could use the services of specialized e-mail suppliers. But, even into this case, under the circumstances of the augmented phenomenon of international terrorism, the state's competent authorities might request from the e-mail suppliers a partial or total monitoring of e-mail correspondence, regarding either individuals or moral persons.

However, if an increased protection is aimed for someone's correspondence, specialized programs able to encrypt the respective messages might be used.

In Great Britain, the employers are entitled, since 2000, to open their subordinates' emails, with no necessity for an authorization previously given by the messages' forwarder or recipient[13].

BIBLIOGRAPHY:

1. Bizeul, B., *Le télé-achat et le droit des contrats*, Editura CNRS Droit, Paris, 1998
2. Brooks, D.T., *Introduction to Computer Law*, New York, Practising Law Institute, 1985
3. Deprez, P., Fauchoux, V., *Lois, Contrats et Usages du Multimédia*, Editura DIXIT, Paris
4. Dogaru Ion, *Drept civil român. Idei producătoare de efecte juridice*, Editura All Beck, Bucureşti, 2002 (author and coordinator)
5. Dogaru Ion, *Filosofia dreptului. Marile curente*, Editura All Beck, Bucuresti, 2002
6. Dogaru Ion, *Drept civil. Teoria generală a obligațiilor*, AllBeck, Bucuresti, 2002 (first author)
7. Dogaru Ion, *Drept civil. Ideea curgerii timpului şi consecințele ei juridice*, Ed. All Beck, Bucuresti, 2002 (author and coordinator)
8. Dogaru Ion, *Drept civil. Teoria generală a drepturilor reale*, Ed. All Beck, Bucureşti, 2003 (first author)
9. Dogaru Ion, *Drept civil. Contractele speciale*, Tratat, Editura All Beck, Bucureşti, 2004 (author and coordinator)
10. Dogaru Ion, *Drept civil. Teoria generală a actelor juridice civile cu titlu gratuit*, Editura All Beck, Bucureşti, 2005 (author and coordinator)
11. Dogaru Ion, *Teorie şi practică în materia titlurilor comerciale de valoare*, Ed. Didactica si Pedagogica, Bucureşti 2006
12. Dogaru Ion, *Teoria generală a obligațiilor comerciale*, Editura Didactica si Pedagogica, Bucureşti, 2006
13. Dogaru Ion, *Teoria generală a obligațiilor comerciale. Jurisprudența*, Editura Didactica si Pedagogica, Bucureşti, 2006
14. Dogaru Ion, Popa Nicolae, Dănişor Dan Claudiu, Cercel Sevastian (coordinators), *Bazele dreptului civil*, vol. I, *Teoria generală*, Editura C. H. Beck, Bucureşti, 2008
15. Dogaru Ion, Stănescu Vasile, Soreață Maria Marieta (coordinators), *Bazele dreptului civil*, vol. V, *Succesiunile*, Editura C. H. Beck, Bucureşti, 2009
16. Dogaru Ion, Drăghici Pompil (coordinators), *Bazele dreptului civil*, vol. III, *Teoria generală a obligațiilor*, Editura C. H. Beck, Bucureşti, 2009
17. Dogaru Ion, Olteanu Gabriel Edmond, Săuleanu Lucian Bernd (coordinators), *Bazele dreptului civil*, vol. IV, *Contracte speciale*, Editura C. H. Beck, Bucureşti, 2009
18. Dogaru Ion, *Teoria generală a dreptului*, Editura C.H. Beck Bucureşti, 2006 (coauthor)
19. Dogaru Ion, *Drept civil. Partea generală*, Editura C.H. Beck Bucureşti, 2007 (first author)
20. Dogaru Ion, *Drept civil. Persoanele*, Editura C.H. Beck Bucureşti, 2007 (first author)
21. Dogaru Ion, *Teoria generală a dreptului*, Ediția a 2-a, Editura C.H. Beck Bucureşti, 2008 (coauthor)
22. Dubisson, M., *La negociation des marchés internationaux*, Editura Moniteur, Paris, 1982
23. Hanga, V., *Calculatoarele în serviciul dreptului*, EdituraLumina Lex, 1996

[13] Regulation of Investigatory Act, October 24-th, 2000

24. Hervier, G., *Le commerce électronique. Vendre en ligne et optimiser ses achats*, Editura Organisation, Paris, 2001
25. Klander, L., *Anti hacker - Ghidul securității rețelelor de calculatoare*, Editura ALL, 1998
26. Lawrence, Penelope, *Law on the Internet. A practical guide*, Editura Sweet & Maxwell, Londra, 2000
27. Lucas, A., Deveze, J., Frayssinet, J., *Droit de l'informatique et de l'Internet*, Editura Themis, Paris, 2001
28. Piette-Coudol, Th., Bertrand, A., *Internet et la loi*, Editura Dalloz, Paris, 1997
29. Popa Nicolae, *Teoria generală a dreptului*, 8 ediții, prima în anul 1992, ultima în anul 2005, Editura All Beck
30. Popa Nicolae, *Drept civil. Ideea curgerii timpului şi consecințele ei juridice*, Editura All Beck, 2002, (coauthor);
31. Popa Nicolae, *Drept civil. Contractele speciale*, Editura All Beck, 2004, (coauthor)
32. Popa Nicolae, *Jurisprudența Curții Constituționale şi Convenția Europeană a drepturilor omului*, Editura Monitorul Oficial, 2005 (coauthor);
33. Popa Nicolae, *Teoria generală a dreptului* (Sinteze pentru seminar), Editura All Beck, 2005 (coauthor).
34. Popa Nicolae, *Jurisprudența Curții Constituționale a României şi Convenția Europeană a Drepturilor Omului*, Ed.Monitorul Oficial, 2005 (coauthor);
35. Popa Nicolae, *Le rapport juridique; Despre constituție şi constituționalism*, vol. Liber Amicorum, I. Muraru, Ed. Hamangiu, 2006
36. Sedalian, V., *Droit de l'Internet*, Editura Netpress, Paris, 1997
37. Smith, G., *Internet Law and Regulation*, Ed. Sweet&Maxwell, Londra, 2002
38. Tourneau, Ph. le, *Théorie et pratique des contrats informatiques*, Editura Dalloz, Paris, 2000
39. Viricel, A., *Le droit des contract de l'informatique*, Editura Moniteur, Paris, 1984
40. Vivant, M., *Lamy informatique*, Editura Litec, Paris, 1989
41. Vivant, M., Stanc, C. le, Rapp, L., Guiball, M., *Lamy droit de l'informatique*, Paris, Lamy, 1992