“ILLEGALLY OBTAINED EVIDENCE AND THEIR USE IN CIVIL PROCEDURE”

BY REVOLIDIS IOANNIS

I. Generalities

"*A theologian asked an almighty computer if there's a God. The computer answered that it didn't have the necessary processing capacity to know. He asked to have it connected to all other supercomputers of the world. But still it was not powerful enough. So, they connected the computer to all host computers, micro-computers and personal computers. Finally, it managed to connect to car computers, microwaves, digital clocks etc. The theologian asked for the last time if there's a God. The computer answered: Now there is!*". The semiotics of this story originating from the mid 90's, can be found in fears as well as in expectations arisen worldwide from the explosive rise and wide spread of electronic networks. Many of the expectations of that time have been fulfilled, yet many of the fears as well were proven to be true, which today are even some of the most important challenges for the Law and not only.

In the early 70's when the modern world entered the third phase of the industrial revolution, in which the digitalization of information data started rising gradually, mainly concerning activities involved in administrative or military organization of most societies but also concerning scientific research, no one could have predicted that modern social aggregations would increasingly depend on electronic communication networks. This event was roughly called "*digital industrial revolution"* and its growth during the years that followed, posed new social issues and new social challenges. The personal computer was no longer only part of the user's little world at his office, nor part only of the limited local network of a business or research team. It became by then a means to enter the global information highway of internet.

Internet fulfilled and implemented at a great extent the basic demand of the western societies (mainly after 1989 and after the collapse of the actually existing socialism) for the transition to an increasing globalized traffic of goods and delivery of services. The ability for people to enter the cyberspace from any continent of the planet, as well as the establishment of transaction contacts where the physical presence of their subjects was not any longer requested has profoundly changed the traditional value framework of the markets. Like any revolution, the digital revolution was accompanied by far reaching reforms in everyday life. The new-fashioned information society is now an international social forum. In this new globalized framework the privacy of individuals became vulnerable in many ways. Without realizing it in its full extent, individuals leave nowadays their digital traces during any kind of their actions, often exposing their private life to an extremely broadened social space. This issue couldn't be of no consequences on the regulatory action of most societies in which it occurred.

The issue of legal regulation of information society has been raised by realizing almost at the same time the wide spread of information. Law reacted rather instinctively and confused. The particularity of information society and especially (in relation to the traditional social phenomena) the different manifestation of most of its aspects (such as the ability to incorporate new and continuously developing technology as well as the ability for individuals from different social groups to participate in it), has triggered a new, for the legal system, kind of discussion regarding its regulation. The standpoints covered the entire range of spectrum beginning from one end, namely considering the information society as a space

outside the law regulating by itself any arising conflicts, and reaching the other end, namely the suffocating supervision and strict control of information society by the respective legal order in which it was manifested. In-between standpoints considered that the particularities of information society do not reach the point of disputing the value and usability of the traditional legal framework, which with the necessary interpretive adjustments, could be applied on the information society as well.

In respect of the character that should be assigned to the regulation of information society by the law, the above mentioned standpoints soon moved on to the civil procedure level (in Europe as well as internationally), where the conflict of fundamental rights and questioning of traditional legal values began to show within the question of illegally obtained evidence. In fact, the question raised on that level was more serious since the conflict of fundamental rights did not exist as an in abstracto discussion but as an in cocreto problem of the entire system of the administration of justice.

Now, how should procedural legal order react when the only evidence introduced to a civil court, is obtained illegally and especially through invasion of the individual's privacy by the parties through the internet? Following must preliminary be noted: a) the above problem does not have the same gravity when the illegally obtained evidence is not the only available evidence but is part of a number of evidence introduced by the parties. The judge can then legally base its conclusion on the remaining evidence, even if the judge practically did take into consideration the illegally obtained evidence and b) theories that consider information society as a space functioning outside the law could not be taken into consideration, since it is not certain that they could provide solutions to the problem in question.

II. The arising problem.

As mentioned above, the science of civil procedural law has already faced in the past the problem of illegally obtained evidence. This rather old question gets new dimensions in the information society. The particularity of the digital environment of internet as well as its global range penetration has intensified the concern on the protection of privacy, given the fact that it was now easier than ever to obtain personal data from one of the parties. Email services, social networking sites, E-market web-pages, electronic forums and blogs are only some of the digital spaces visited by millions of users every day. At each visit the users leave digital traces and data of personal nature that compose together their personality. The creation of "digital profiles" is therefore is quite often, based on websites visited by an internet user. The easy way by which an individual can be identified (e.g. though the IP address of its personal computer or its email), as well as the relevant ability to supervise the visited websites, verify without much of a doubt, how easy it is today to intrude the privacy of the subjects in information society. This penetration and gathering of personal data resulted thereby, is being used not only for private or commercial purposes but today also for purposes of a civil court, since often one of the opposite parties manages to detach private information of the other party, which could be decisive for the procedure outcome.

Following cases, which reached the Greek Courts, demonstrate the real dimension of the problem. It is worth noticing that the facts of the cases have been simplified in order not to put into question the breach of the parties' personal data:

First example: In order for A, husband of B, to support a legal action filed against her in order to obtain dissolution of their marriage by exclusive liability of the wife, he introduced at the hearing and submitted at the court electronic letters sent and received from the electronic mail address of his wife. According to the opinion of the plaintiff A, the content of those letters was erotic and proved that his wife had an affair with another man. It is noted that A did not obtained any consent from his wife B to access her email account, nor did he obtained her consent to detach these particular letters. At the same time, this specific email account belonged exclusively to his wife and was not a common use account.

Second example: The second case deals with posting of personal information of one of the parties on a social networking site by the other party. In particular, A was a teacher at the department of journalism and mass media of a university and at the same time candidate for a position in the scientific teaching personnel as a assistant professor or associate professor in the cognitive field "Journalism: social and cultural coverage" announced at the same institution. The position in question was initially announced at the end of 2005, so A had submitted a complete candidacy file containing all documents related to her academic, journalistic and professional career. Finally, the procedure ended with no result and the position was announced at new in 2008. While the new announcement was still pending, in October 19th 2008 various texts were posted on the website "facebook.com" on a special area created by an unknown user with the alias-name "P.P" und under the title "H.P. and all the friends". In these texts the unknown author used insulting comments on A, questioned her degree titles (master and doctor degree) and claimed that she was acting under the orders and was close friend of an assistant professor of the department, who would illegally promote her to receive the announced position (as claimed by the unknown author). Further on new slanderous texts on A were posted, sent also as electronic messages to a list of approximately three hundred (300) electronic addresses of individuals who were academics, politicians and journalists. B was an assistant professor at another educational institution and co-candidate of A for the above mentioned position. On November 10th 2008 he submitted to the secretary office of the department of journalism at the aforementioned institution a request and by claiming a number of publications on the internet "with complaints against his opposing candidate (namely A) for the position of the associate – assistant professor, he asked to receive as soon as possible copies of 1. all her study degrees submitted to the secretary of the department, 2. all certificates issued by the Hellenic National Academic Recognition and Information Center concerning the recognition of those degrees, 3. all certificates of her vocational occupation, 4. her doctoral degree, 5. her teaching notes and 6. the text of her lecture at Harvard University. In order to obtain the aforementioned copies, he claimed legal interest in his capacity as a co-candidate of applicant A for the announced position. At the end of his application he noted: "If my co-candidate requests a copy of any of the documented contained in my candidacy file, please provide it to her without any delay and as soon as possible as stipulated by law". On the same day by submitting another request to the Rector of the educational institute, he protested because the head of the secretary office of the department of journalism refused to furnish the requested documents, claiming that he should prior speak on the telephone to the vice-chairman or the chairman of the department, which was impossible to take place on that day. He also spoke about an intentional and illegal "manipulation". When A learned about the request of B, she decided to give him herself the requested documents. Therefore, she asked a final-year student to

deliver a batch of documents to an employee of the secretary office and this employee should further on deliver the documents to B by signing a delivery receipt of the documents. Prior to the delivery of the documents to B, a delivery receipt was drawn up stating in a list the delivering documents. All above mentioned documents were contained in the file of the supporting documents submitted by the candidate in 2005 for her candidacy on the announced position, except for some other documents which A copied from her personal file. As soon as the list was drawn up, B came to the secretary office of the educational institution. The employee handed out the documents in a closed envelope and asked B to sign the delivery receipt with the list of the delivering documents. Although B received the envelope, he refused to sign and left. He claimed that the employed handed out to him a closed envelope saying that A sends it and that this envelope contains only some of the documents he requested. However, it was proven that the envelope did contain all aforementioned documents and that B refused to sign the delivery receipt and left. It was also proven that on the same day the pre-mentioned webpage hosted information that was not contained in the file of the year 2005, but only in a document that was delivered to B by A from her personal file. On a following day, documents that were included in the file of 2005 delivered by A to B were posted on the internet. Together with those documents, the documents that were not contained, as already mentioned, in the candidacy file of 2005 but were delivered to B by A, were also posted on the internet. Later on nine (9) more documents from the file of 2005 were posted, while a bulk email to the aforementioned group of the three hundred (300) recipients sent by the unknown P.P, contained letters of reference delivered by A to B. At the end, the same webpage hosted the university notes of A, which were never published nor were ever distributed to students. In fact, they were contained only in her file and in a copy in the candidacy file of 2005. Please note, that no one else expressed any interest in obtaining copies of the pre-mentioned documents. So the only one that could have them was B. It was proven that he did post all the documents concerning the employment conditions and the professional career of A, without her consent. A delivered B the documents only as an information since he was her co-candidate. In fact these postings on the specific webpage, where anyone could have access to (especially by the search machine where the user could write the name of A and be led automatically to this webpage), were at the same time a violation of A's privacy, since there were accompanied by inappropriate and demeaning sentences (e.g. here are the Greek references on our A") and gave the impression that they were proof of the fact that the degrees of A were illegal but also that she had connections to politicians who were helping her. Of course B claimed not to have the required technical knowledge to be able to do on his own the above actions, but the Court was convinced that the postings was an act of A himself by using a person with the necessary technical knowledge. It is noted that B, though he received the document file only for his personal use, he showed them at least to the witness who testified at the court hearing on his initiative (legal right of B).

In the above example cases, one of the parties violated through the internet, the personal data of the other party and obtained in this way evidence. The question raised, focuses on whether illegally obtained evidence implies procedural inadmissibility in a civil court.

III. Suggested solutions.

The question if substantial illegality could be transformed into procedural inadmissibility when one of the parties violates the privacy of the other party through the internet is not addressed always in the same way. We must not ignore, that in the entire discussion the different approach of the various legal orders in relation to the regulation of information society plays a key role. As long as a legal order considers information society to be a space that cannot be regulated by law, it hopes to deal with this problem by relaying on reflexes and self-regulation procedures that could appear inside the information society itself. Other legal orders, on the other hand, choose to regulate by legislative instruments, issues regarding protection of the privacy of the subjects of information society, by taking special measures also for the transformation of the substantial illegality into procedural inadmissibility.

The issue of illegally obtained evidence is an old concern of the Greek civil procedural law. Within the relative question, all possible aspects were supported: a) illegally obtained evidence is not procedurally inadmissible, given that the substantial illegality cannot be transferred to the procedural level. Besides, according to this aspect, in the civil procedure the most important thing is the correct administration of justice, therefore in order to achieve this goal, illegally obtained evidence could be used as well, and b) the illegal character of obtaining evidence, specifies also its procedural use as inadmissible, given that the legal order is consistent, while it was claimed with convincing argumentation that the elevation of the substantial illegality into procedural inadmissibility could not be based only on the issue of the legal order's consistence, but on the aspect that the system itself of the Greek code of civil procedure provided sufficient entitlement.

The establishment of information society, as mentioned extensively, created new challenges and set the discussion on a new basis. These new challenges contributed to the realization of the newly arisen need to create new rights which could apply in the civil procedure as well. In 2001 the legislator in revising the Constitution, took into consideration the new arisen needs and adopted significant substantial rights and procedural prohibitions, putting finally an end to the discussion on illegally obtained evidence. It is worth noticing, that despite the fact that the new rights could be concluded from already existing regulations of the Greek Constitution, the legislator preferred to explicitly establish the rights, so that especially the Greek legal order can adjust to the continuously changing and in all times unforeseen challenges arisen by the participation of individuals in the information society. The establishment of the new rights was not only a confirmation but prevention as well. In virtue of the new clause 9A and the two new sub-clauses added to clause 19, the Greek constitution explicitly guarantees the protection of personal data against collection, processing and use though electronic means, as well as through non-electronic means. At the same time it clearly forbids, before any court (civil, criminal, administrative) or instrument and in any procedure, the use, by any means, of evidence obtained by illegal processing of personal data or by violating the confidentiality of responses. The constitutional legislator has established the fact that the protection of personal data as well as the protection of the confidentiality of responses would be rather worthless if not accompanied by its corresponding procedural dimension. The protection would not be complete if the illegally obtained material could be used without any hindrance before civil courts (and before any other court). The right of informational privacy established by clause 9A of the Constitution, is thusly procedurally secured by the regulation of clause 19 19 § 3. The

constitutional prohibition to use illegally obtained evidence in a civil court by virtue of clauses 9A and 19 § 3, corresponds legislatively and meets the conditions for its consistent practical appliance, to the provisions of law 2472/1997, by which Greece has incorporated into its domestic law the Directive 95/46 EC of the European Parliament and Council regarding the protection of individuals against processing of personal data and the free circulation of this data. Only then is allowed to use evidence obtained by collecting and using personal data, when the collection and use do not constitute a breach of clauses 4, 5, 7 and 7A of law 2472/1997, regulating the conditions of legitimate processing of personal data. Therefore, when a data is subject to the appliance field of law 2472/1997 and hence is a personal data (for non personal data, the evidence prohibition may result from other constitutional provisions protecting the fundamental rights or from provisions of the civil procedure code, the question if it can be used before a civil court can be answered under following regulatory condition: if it is a "simple" personal data, the carrier of the personal data can consent to its collection and processing. At the same time, for this particular category of personal data, as an exemption the collection and processing is allowed even without the consent of the carrier, provided that the, in law 2472/1997 restrictively documented exemptions are concurrent. For example, pursuant to clause 5 sub-clause 2, section ε΄ of law 2472/1997, the processing of the subject's data without consent, when it is absolutely necessary in order to satisfy the legal interest endeavored by the responsible person for the processing or the third party or parties to whom the data is announced and under the self-evident condition that the need for processing has more gravity in relation to the rights and fundamental constitutional freedoms of the individuals being processed. In short, the exceptional processing of personal data of an individual without its consent for the satisfaction of the legal interest of the responsible person for the processing, can take place only if it is absolutely necessary and obviously more important than the interests and fundamental freedoms of the processed subject. As to the "sensitive" personal data (clause 7 law 2472/1997), on the contrary, the legislator's regulation is indeed more strict. In this case, the collection and processing of data is forbidden and is tolerated only by exemption, upon relative permission given by the Hellenic Data Protection Authority and provided that the terms of § 2 clause 7, law 2472/1997 apply. However, the above protective framework becomes relative through the regulation of clause 7A law 2472/1997, which allows the processing of "sensitive" personal data without the permission given by the Hellenic Data Protection Authority when one of the cases documented in its second sub-clause is concurrent.

For the problem under discussion it is very interesting to mention the regulation of clause 7 § 2 section. γ΄of law 2472/1997, which foresees following: "… *Exceptionally, the collection and processing of personal data is allowed when …: c)the processing relates to data published by the subject itself or when the processing is necessary in order to acknowledge, exercise or defend a right before a court or a disciplinary instrument* …". Pursuant to the dominating opinion, this provision applies also on the simple personal data, in virtue of the interpretive principle from major to minor, with the particularity that in the case of "simple" personal data, it is not necessary to obtain a permission by the Hellenic Data Protection Authority for processing data. The importance of the regulation for the field of civil court is significant, since the legislator attempts in this way to combine the conflict of the parties' fundamental right of evidence with the compelling need to protect the privacy of individuals. It is worth mentioning, that even if the processing of simple or sensitive personal data is allowed without the subject's consent in order for the

responsible person of the data processing to defend its right before a civil court, the processing is still subject to the limitation of the purpose and necessity: it shall be allowed to process data only to the extent needed to fulfill the purpose of defending a right before a civil court. Any processing exceeding this limit shall be automatically considered as illegal and thusly leads immediately to an procedurally inadmissible evidence

The, in advance, limited territorial range of a spatially finite legal order, however, cannot cover the needs of privacy protection in the modern globalized framework of information society. The European Union, by realizing relatively soon this problem, took action in order to uniform the level of privacy protection on a community level, in an attempt to exceed beyond any spatial limits set by the classical private international law. The result of this attempt was the fundamental Directive 95/46 EC of the European Parliament and Council regarding the protection of individuals against processing of personal data and the free circulation of this data. This Directive, despite the compelling need for its modernization and adjustment to the new technology data, remains a basic flag of the community law in terms of privacy protection. In information society, the protection of privacy is completed by the directives 2002/58/EC and 2006/24/EC. At this point we must also mention the significant contribution of the Lisbon Convention in the attempt to secure private life from external (electronic or non-electronic) violations. Bu clause 6 of the Convention, the Map of Fundamental Rights of the European Union has a binding effect for the state members. Clauses 2,7 and 8 of the Map of fundamental Rights establish the protection of the human value as well as the protection of the individual's private and family life, while the protection of personal data from external violations is also explicitly established. The contribution of the Court of the European Community (already Court of the European Union) has been very important in terms of securing private life from violations taken place in information society. In virtue of the fundamental resolution **Bodil Lindqvist** (case C – 101/2001), the Court ruled already at the beginning of the past decade, that the posting of personal data on the internet is an illegal processing of personal data. Though the above regulatory provisions and the currently valid decisional law of the Court of the European Union did not deal with matters of procedural character, we would dare to say that the fundament for the dogmatically smooth transition from the substantial illegality to the procedural inadmissibility has been set. The key importance contributed to the protection of privacy as well as the increased level of protection set by the existing community institutional framework, would justify rather a dogmatic attempt in the direction to an (at least) interpretative modernization of the legal categories "substantial illegality" and " procedural inadmissibility". The protection of privacy in information society would not seem to be complete if it has no procedural correspondence. The unconditional violation of personal data during a court proceeding would leave a wide field of breaching the community law regarding the protection of privacy and would drastically harm its effectiveness. The unification of the level of the protection of personal data in Europe must inevitably pass through the procedural path.

Though the European institutional framework provides more or less sufficient entitlement for the protection of personal data on the level of substantial law and procedural law as well, the question if this applies also globally, remains unanswered. Like most of the national legal orders, the European legal order as well sets specific spatial boundaries, which drastically limit the effect of the community legislative instruments. The appliance of Directive 95/46/EC cannot stand outside the European Economic Area. The globalized dimension of information society often poses the

question of processing personal data of individuals residing in Europe, by persons responsible for data processing established in other geographic continents. Besides, equally often, the level of personal data protection in countries where the processing takes place is not proportional to the one encountered in the European Union. At the same time, the means of classical private international law seem not to provide satisfactory solutions when seeking an international jurisdiction of the legal order which shall rule on the cases of personal data processing: every time the means of classical private international law shall result in affirmation of international jurisdiction of a legal order where the level of the protection of privacy is weak, the legislative armory of legal orders which took measures for its substantial and procedural protection shall lose its meaning. The achievement of the goal to protect individuals being violated by third parties in their private life, a goal set by most of the legal orders of the western world, presupposes the interpretive transformation of traditional value constants of the private international law (at least as long as the international cooperation and the effort to create a common international protection framework do not result in practically useful outcomes), in a direction that leads to a best possible protection of privacy. The more substantial and procedural guarantees a legal order offers, the more the interpreter and applier of law should ensure to choose it in order to decide on a personal data processing case. The judgment on international jurisdiction, as already ruled by a explicit legislative intervention for other cases of preventive substantial regulation (see clauses 8 f., 15 f., and 18 f. EC 44/2001), must be led by the increasing need to protect the human value and personal data.

IV. Instead of an epilogue

The value of the human personality and privacy of individuals, a domain of the liberal social revolutions that took place in the past centuries, is unrestrained put in question by the new challenges of information society. The easy way by which third parties can intrude the privacy of individuals and detach any kind of personal information, makes the privacy of subjects in information society vulnerable in many ways, while the self-regulating reflexes of information society seem not to be evolved to the extent needed to ensure a substantially and procedurally complete and critical protection of personal data. The illegally obtained evidence regarding the privacy of one of the parties and the use of it, has a new globalized dynamics. The overall awareness and legal regulation of such dynamics cannot take place within an environment of national or regional isolation. The classical dogmatic constants of private international law, but also the fundamental right of evidence are put in question by the existential conflict with the increasing need to protect privacy. The interpretive release of the intensity and conflict field of those rights in the light of technology in information society, is a challenge that belongs to the future.

Selected Literature

- Ανθόπουλος Χ. (1993), Το πρόβλημα της λειτουργικής δέσμευσης των θεμελιωδών δικαιωμάτων.
- Αρκουλή Κ. (2010), Προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.
- Βενιζέλος Ευ. (2002), Το αναθεωρητικό κεκτημένο. Το συνταγματικό φαινόμενο στον 21ο αιώνα και η εισφορά της αναθεώρησης του 2001.
- Γέροντας Α. (2002), Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων.
- Γέσιου – Φαλτσή Ν. (1985), Δίκαιο Αποδείξεως.
- Δαγτόγλου Π. (1991), Συνταγματικό Δίκαιο – Ατομικά και Κοινωνικά Δικαιώματα Α΄και Β΄.
- Δημητρόπουλος Α. (2002), Το Σύνταγμα ως βάση της έννομης τάξης.
- Δόνος Π./Μήτρου Λ./Μίτλεττον Φ./Παπακωνσταντίνου Ευ. (2002), Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων.
- Ζέρη Περσ. (1999), Κρατική ρύθμιση και αυτορρύθμιση των υπερλεωφόρων των πληροφοριών, ΝοΒ, 47, σ. 407.
- Ιγγλεζάκης Ι. (2003), Ευαίσθητα προσωπικά δεδομένα.
- Ιγγλεζάκης Ι. (2004), Δημοσιοποίηση και διαβίβαση προσωπικών δεδομένων μέσω του Διαδικτύου, ΔιΜΕΕ, 1, 498.
- Ιγγλεζάκης Ι. (2010), Παράνομα αποδεικτικά μέσα. Επιστολές μέσω του διαδικτύου, ΔιΜΕΕ, 6, 401.
- Καΐσης Αθ. (1986), Παράνομα αποδεικτικά μέσα.
- Καλαβρός Κ. (1991), Η μαγνητοταινία στην πολιτική δίκη.
- Καμίνης Γ. (1998), Παράνομα αποδεικτικά μέσα και συνταγματική κατοχύρωση των ατομικών δικαιωμάτων.
- Καράκωστας Ι. (2001), Δίκαιο και Ίντερνετ – Νομικά ζητήματα του Διαδικτύου.
- Κική Γ. (2003), Η ελευθερία των οπτικοακουστικών μέσων (υπό το πρίσμα και της συνταγματικής αναθεώρησης του 2001).
- Κόμνιος Κ. (2010), Η νομιμότητα διαδικτυακών εφαρμογών τρισδιάστατης χαρτογράφησης και εικονικής περιήγησης (Google Street View), ΔιΜΕΕ, 6, 170.
- Κουσούλης Στ. (1992). Σύγχρονες μορφές έγγραφης συναλλαγής (Telex – Telefax – Ηλεκτρονικό έγγραφο).
- Μάνεσης Αρ. (1982), Συνταγματικά Δικαιώματα, α΄ ατομικές ελευθερίες.
- Μανιτάκης Α. (2001), Συνταγματική οργάνωση του κράτους, Κράτος – Έθνος – Σύνταγμα – Κυριαρχία – Παγκοσμιοποίηση.
- Μανωλεδάκης Ι. (2003), Ελευθερία και Ασφάλεια.
- Μήτρου Λ. (1999), Η αρχή προστασίας προσωπικών δεδομένων.
- Μήτρου Λ. (2001), Το δίκαιο στην κοινωνία της πληροφορίας.
- Μήτρου Λ. (2009), Ανάρτηση στο facebook εγγράφων με προσωπικά δεδομένα και δυσφημιστικών σχολίων, ΔιΜΕΕ, 5, 400.

- Μήτρου Λ. (2010), Η ιδιωτικότητα στο web 2.0, ΔιΜΕΕ, 6, 319
- Μητσόπουλος Γ. (2002), «Τριτενέργεια» και «αναλογικότητα» ως διατάξεις του αναθεωρηθέντος Συντάγματος, ΔτΑ, σ. 641.
- Μπέης Ευ. (2001), Παραδεκτό επίκλησης μαγνητοφώνησης ιδιωτικής συζήτησης που διενεργήθηκε δίχως τη συναίνεση του συνομιλητή, Δίκη, 32, 519.
- Νίκας Ν./Διαμαντόπουλος Γ. (2004), Η δυνατότητα χρήσεως στην πολιτική δίκη αποδεικτικών μέσων που αποκτήθηκαν παράνομα, ΕλλΔνη, 44, 694.
- Νίκας Ν. (1999), Σχετικά με το επιτρεπτό των αθεμίτως κτηθέντων αποδεικτικών μέσων, Νομικές Μελέτες, 251.
- Νικολόπουλος Γ. (2005), Το δίκαιο της αποδείξεως.
- Ορφανουδάκης Σ. (2003), Η αρχή της αναλογικότητας στην ελληνική έννομη τάξη. Από τη νομολογιακή εφαρμογή της στην συνταγματική της κατοχύρωση.
- Παναγοπούλου – Κουτνατζή Φ. (2010), Οι ιστότοποι κοινωνικής Δικτυώσεως ως Εθνική, Ευρωπαϊκή και Διεθνής Πρόκληση της Ιδιωτικότητας.
- Παρασκευόπουλος Ν. (2002), Το δίκαιο μπροστά στην πρόκληση της παγκοσμιοποίησης.
- Πισκοπάνη Α – Μ. (2009), Η προστασία της ιδιωτικότητας των χρηστών του facebook, ΔιΜΕΕ, 5, 338.
- Τάκης Α. (2002), Κοινωνία της πληροφορίας και Σύνταγμα, ΝοΒ, 51, 28.
- Τσόλιας Γ. (2006), Η διατήρηση και επεξεργασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών σύμφωνα με την Οδηγία 2006/24/ΕΚ, ΔιΜΕΕ, 3, 347.
- Χρυσόγονος Κ. (2006), Ατομικά και Κοινωνικά Δικαιώματα.
- Allen A. (1988), Uneasy access, Privacy for women in a free society.
- Alivizatos N. (2001), Privacy and transparency: A difficult conciliation.
- Benabou Valerie – Laure (2001), Should there be a minimum harmonization of the law?, online at http://droit-internet-2001.univ-paris1.fr/ve/page004.html\ accessed 22.03.2011.
- Benn St. (1971), Privacy, Freedom, and Respect for Persons.
- Bloustein E. (1964), Privacy as an Aspect of Human Dignity: An answer to Dean Prosser, N.Y.U.L Rev., 39, 962.
- Brandenburg C. (2008), The newest Way to Screen job Applicants: A social Networker's Nightmare, Fed. Comm. L. J., 60, 597.
- Cheh M. (2001), Technology and privacy: Creating the conditions for preserving Personal Privacy.
- Choo Andrew L – T. (1989), Improperly obtained evidence: a reconsideration, Legal Studies,9, 261.
- Fatouros A. (2001), Technological Development, Human Rights and Cultural Diversity, in: Linos Alexandros Sicilianos and Maria Gavouneli (editors), Scientific and Technological Developments and Human Rights.
- Gavison R. (1980), Privacy and the limits of Law, Yale L.J., 89, 421.
- Giddens Anthony, Κοινωνιολογία (2002).
- Giddens Anthony (2001), Οι συνέπειες της νεωτερικότητας.
- Hashemi Y. (2009), Facebook's privacy policy and its third-party partnerships, B.U.J.SCI. & Tech. L., 15, 140.

- Kang J. (1998), Information Privacy in Cyberspace Transactions, Stan. L. Rev., 50, 1193.
- Guo R. M. (2008), CYBERLAW: Note: Stranger Danger and the Online Social Network, Bekerley Tech. L.J., 23, 617.
- Katsh M.E. (1995), Rights, Camera, Action: Cyberspatial settings and the First Amendment, Yale Journal Law, 104, 1690.
- Lessig L. (1996), Reading the Constitution in Cyberspace, Emory Law Review, 45, 861.
- Lessig L. (1998), The Laws of Cyberspace.
- Millier S. L. (2009), The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet, K.Y.L.J., 97, 541.
- Sykes Ch. (1999), The End of Privacy: The attack on Personal Rights at home, at work, Online.