Activity Report 2011

Exploratory Action LICIT

Legal Issues in Communication and Information Technologies

RESEARCH CENTER
Grenoble - Rhône-Alpes

Table of contents

Exploratory Action LICIT

Keywords: legal, Law, Liability, Privacy, Obligation, Evidence, Contract, Formal, Model, Software, Log

1. Members

Research Scientist

Daniel Le Métayer [Team Leader, Senior Researcher, INRIA, HdR]

PhD Students

Thibaud Antignac [since September 2011]
Sophie Guicherd [with University Pierre Mendès-France]
Eduardo Mazza [with VERIMAG]

Administrative Assistant

Françoise De Coninck

2. Overall Objectives

2.1. Introduction

The main objective of LICIT is to undertake new research activities on the interactions between ICT and the law. The motivations for this new initiative are manifold. First and foremost, the rapid evolution of the technological landscape and the impact of ICT on the everyday life of citizens (including their private lives) raise new challenges which cannot be tackled by a purely technological approach [17]. For example, the protection of privacy rights on the Internet or in pervasive computing environments is by definition multidimensional and requires expertise from disciplines such as social sciences, economics, ethics, law and computer science [19]. Other examples of the ever-growing intermingling of ICT and law include electronic commerce, digital rights management (DRM), social networks, forensics, cybercrime, e-government, and e-justice. As far as research is concerned however, there are still very few links between the ICT and law communities. This situation is unfortunate considering the importance of the interests (both societal and economical) at stake. In addition, at a time of growing mistrust of citizens towards technology, more attention should be paid to the implications of research results on society.

Starting from this observation, the goal of LICIT is to contribute, in partnership with research groups in law, to the development of new approaches and methods for a better integration of technical and legal instruments [7].

In practice, the interactions between ICT and law take various forms and go in both directions [14]:

- The ICT "objects" are, as any other objects, "objects of law": on one hand, there is no reason why new technologies and services should escape the realm of law; on the other hand, it may be the case that existing regulations need to be adapted to take into account the advent of new, unforeseen technological developments (e.g. certain provisions of privacy regulations become inapplicable in a pervasive computing context, intellectual property laws are challenged by the new distribution modes of electronic contents). Understanding precisely when this is the case and how regulations should evolve to cope with the new reality may be a complex "technico-legal" issue with potential impacts on both disciplines.
- ICT can also provide new enforcement mechanisms and tools for the benefit of the law. For example, DRM technologies are supposed to "implement" legal provisions and contractual commitments, Privacy Enhancing Technologies (PET) help reduce privacy threats, certified tools can be provided to support electronic signature, computer logs can be used as evidence in courts, etc. At a different level, data mining or knowledge management systems can be applied to the extraction of relevant legal cases or the formalization of legal reasoning.

Generally speaking, legal and technical means should complement each other to reduce risks and to increase citizens' and consumers' trust in ICT: on one side, laws (or contracts) can provide assurances which are out of reach of technical means (or cope with situations where technical means would be defeated); on the other side, technology can help enforce legal and contractual commitments. This synergy should not be taken for granted however, and if legal issues (and more generally, the consequences of the technologies on society) are not considered from the outset, technological decisions made during the design phase may very well hamper or make impossible the enforcement of legal rights.

In the longer term, further thought needs to be devoted to the potential conflicts between, on one side, rapidly evolving technologies and, on the other side, bodies of regulations which, in essence and for the sake of "legal security", require a form of stability. This complex issue is related to the problem of finding the right level of abstraction in regulations - or strike the right balance between very general principles (which remain stable but offer little indication as far as practical application is concerned, and can thus lead to another form of legal insecurity) and precise provisions whose application may be less prone to interpretation but are bound to become quickly outdated.

The means used by LICIT to reach its objectives are twofold:

1. Research actions: to investigate specific research topics following an interdisciplinary approach in order to better integrate legal and technical instruments. This research work emphasizes the use of formal methods as a link between the ICT and regulations.
2. Networking actions: to favour the emergence of an "ICT and law" research community and to enhance the interest of ICT researchers in this emerging field.

The outputs of the first line of actions are research results whereas the networking actions take the form of joint events (seminars, conferences), joint projects and position papers.

2.2. Highlights

The main results of the year concern both the aforementioned research and networking objectives:

- Integration of technical and legal requirements in a common framework to reduce legal uncertainties in software liability [5].
- Definition of a formal language for the specification of obligations and *a posteriori* verification of legal rules [10].
- Co-organization of a multidisciplinary conference on digital evidence (Palais de Justice de Paris, 8 December 2011) [1].
- Organization of a multidisciplinary workshop on legal and technical aspects of causality (ENSCP Paris, 7 December 2011) [2].
- Co-organization of the CPDP Conference and panel on "behavioural targeting" [3]. CPDP, which is now established as the main privacy conference in Europe, attracts every year a wider and more multidisciplinary audience (more than 300 participants in 2011).

3. Scientific Foundations

3.1. Formal methods as a link between ICT and law

Beyond their many differences, ICT and law share a strong emphasis on formalism. This commonality is not without reason: in both cases formalism is a way to avoid ambiguity and to provide the required level of rigour, transparency, and security. As an illustration, L. Fuller in his book "The morality of law" [13] puts forward the

[1] http://licit.inrialpes.fr/lise/
[2] http://licit.inrialpes.fr/lise/
[3] http://www.cpdpconferences.org

following distinctive features of a legal system: (1) set of rules (2) without contradiction (3) understandable (4) applicable (5) predictable (6) publicized and (7) legitimate. Even though they were obviously not proposed with such a comparison in mind, it is interesting to note that, among these features, the first five are also often used in computer science to characterize a good software specification.

As far as software is concerned, the fact that both disciplines refer to the word "code" is not insignificant and the explorations of the commonalities can be very fruitful (and not only from a theoretical perspective). Indeed, there are many situations where the frontier between the two notions seems to be blurring [4]. Just to take a few examples:

- Software contracts typically incorporate references to technical requirements or specifications which can be used, for example, to decide upon acceptance of the software by the customer or validity of an error correction request. In case of litigation, such specifications can also be used by the judges since they form part of the contract executed by the parties. In this perspective, the contract can thus be seen as an extension of the technical specification including further requirements such as use rights, delivery schedule, warranty, and liability.
- Several languages have been proposed to express privacy policies (e.g. P3P by the W3C Consortium and EPAL by IBM); they are used by some commercial sites and can be handled by popular browsers such as Mozilla Firefox or Internet Explorer. The policies published by these sites can be used both by software code - checked by browsers or enforced by Privacy Enhancing Technologies (PET) - and by judges, possibly interpreting them as commitments on the privacy policy of the company.
- The DRM technologies are supposed to implement legal provisions and contractual commitments about the use of digital content such as music or video.
- More and more transactions are performed on the basis of electronic contracts (SLA: Service Level Agreements for Web and grid services, electronic software licenses, e-commerce contracts, etc.).

In fact, the convergence has developed so much that legal experts have expressed worries that "machine code" might more and more frequently replace "legal code", with detrimental effects on consumers. This topic has stirred up a series of discussions and publications in the legal community [15], [16], [18] and is bound to remain active for quite a long time. Indeed, the implementation of contractual commitments by computer code raises a number of issues such as the lack of flexibility of automated tools, the potential inconsistency between computer code and legal code, the potential errors or flaws in computer code itself or the respective roles of human beings and computers in the process.

The position taken in LICIT is that the first step for a fruitful and useful exploration of the relationships between legal and software code is the definition of a formal framework for expressing the notions at hand, understanding them without ambiguity, and eventually relating or combining them.

3.2. Relevant techniques

The formal methods relevant to LICIT include (1) specification methods and (2) validation methods.

1. Specifications are models or abstract representations of IT systems and their properties which can be used to define their expected behaviour without ambiguity. Specifications can also serve as a basis for various kinds of analyses and tools such as consistency analysis, validation, evaluation, certification, and animation. Specifications can play a role at different phases of the life cycle of a system : before, during or after its design and development. Different specification frameworks have been proposed, which can be roughly classified into semi-formal methods and formal methods. Semi-formal methods provide a well-defined syntax for the models (or "views" of the models) while the underlying semantics remain informal; in contrast, formal methods rely on a mathematical framework which is used to define the semantics of the models. The benefit of semi-formal methods is the definition of a shared body of notions, presentation rules and graphical tools which improve the communication and mutual understanding between the actors involved in the life-cycle of a

[4] Lawrence Lessig refers to East Coast Code and West Coast Code to denote respectively law and software code [16]

system (designer, architect, development teams, evaluators, etc.). However, because of their lack of mathematical semantics, they do not necessarily guarantee the absence of ambiguity and they are not supported by formal verification tools. A standard example of semi-formal framework is UML. In contrast, formal methods such as Coq or B come with interactive theorem provers which help users verifying critical properties of their models. In addition, they provide ways to establish a formal link between a model and its implementation (through program extraction in Coq and refinement in B). Both formal and semi-formal methods are relevant to LICIT, especially specification techniques based on "execution traces" where the expected behaviour of a system is defined in terms of properties of its sequences of operations. As far as logical frameworks are concerned, temporal logics (which make it possible to express properties on the future or the past) and deontic logics (which involve obligation and permission operators) are of prime importance in specifying legal rules.

2. Validation consists in checking a system to ensure that it behaves as expected. The most ambitious validation methods involve a formal specification of the system (using one of the aforementioned formalisms) and a proof (usually interactive) that the actual implementation complies with the specification. An alternative approach is to use the formal specification to derive test suites in a systematic way based on well-defined coverage criteria. The validation can also consist of checking simpler properties (typically well-foundedness properties such as type correctness, absence of buffer overflow or implementation of specific security properties) using automatic tools: these tools are called "type checkers" when the properties to be checked are expressed as types and "program analysers" when they are defined in terms of abstract domains. The main benefit of this category of tools is their automation; their limitation is the restricted expressive power of their language of properties. For LICIT, *a posteriori* verifications are as relevant as *a priori* verifications: *a posteriori* checks are necessary when *a priori* verifications are either insufficient or not feasible, which is the case in particular for obligations which cannot be enforced by technical means.

To conclude this subsection, we stress the fact that the separations into categories (semi-formal versus formal, type inference versus program analysis, testing versus verification) have been used for the sake of the presentation (and because they originated from different research communities) but the frontiers between them tend to blur: for example certain frameworks include semi-formal and formal techniques, graphical representations such as state diagrams can be endowed with formal semantics, types can be defined in terms of abstract domains, program analysers can themselves be checked by theorem provers, etc.

4. Application Domains

4.1. Application Domains

The application areas which are directly concerned by LICIT are varied, including

- Services and products involving the collection or processing of personal data (internet services, location based services, smart metering, cloud computing, pervasive computing, videosurveillance, etc.).
- E-commerce, cloud computing, software licensing, IT contracts (w.r.t. contractual issues, obligations and liability).

5. New Results

5.1. Liability issues in software engineering

Software contracts usually include strong liability limitations or even exemptions of the providers for damages caused by their products. This situation does not favour the development of high quality software because

software editors do not have sufficient economic incentives to apply stringent development and verification methods. Indeed, experience shows that products tend to be of higher quality and more secure when the actors in position to influence their development are also the actors bearing the liability for their defects. The usual argument to justify this lack of liability is the fact that software products are too complex and versatile objects whose expected features (and potential defects) cannot be characterised precisely, and which thus cannot be treated as traditional (tangible) goods. Taking up this challenge is one of our objectives [12] : we study liability issues both from the legal and the technical points of view with the aim to put forward a formal framework to (1) define liability in a precise and unambiguous way and (2) establish such liability in case of incident.

Obviously, specifying all liabilities in a formal framework is neither possible nor desirable. Usually, the parties wish to express as precisely as possible certain aspects which are of prime importance for them and prefer to state other aspects less precisely (either because it is impossible to foresee at contracting time all the events that may occur or because they do not want to be bound by too precise commitments). Taking this requirement into account, we provide a set of tools and methods to be used on a need basis in the contract drafting process (as opposed to a monolithic, "all or nothing" approach). Our model is based on execution traces which are abstractions of the log files of the system. In a nutshell, liability is specified as a function taking as parameters a claim and an execution trace and returning a set of "responsible" actors. This set of actors (ideally a singleton) depends on the claim and the errors occuring in the trace. Both errors and claims are expressed as trace properties. The liability function can be made as precise or detailed as necessary by choosing the claims and errors relevant for a given situation [5].

In order to provide a more generic way to define liabilities, we have also introduced a concept of "logical causality" [11]. Causality has been studied for a long time in computer science, but with quite different perspectives and goals. In the distributed systems community, causality is seen essentially as a temporal property. We have defined several variants of logical causality allowing us to express the fact that an event e_2 (e.g. a failure) would not have occurred if another event e_1 had not occurred ("necessary causality") or the fact that e_2 could not have been avoided as soon as e_1 had occurred ("sufficient causality"). We have applied these technical definitions of causality to real case studies and related them to the legal views of causality.

As far as legal issues are concerned, we have studied the legal validity of the technical solutions proposed in the project both in terms of legal evidence and allocation of liabilities [6]. Contract templates have been defined in collaboration with lawyers to allow the parties to effectively integrate our results in a legal contract [6].

5.2. Privacy

Despite apparently strong legal protections, many citizens feel that information technologies have invaded so much of their lives that they no longer have suitable guarantees about their privacy. As a matter of fact, many aspects of new information technologies render privacy protection difficult to put into practice. A lot of data communications already take place nowadays on the Internet without the users' notice and the situation is going to get worse with the advent of "ambient intelligence" or "pervasive computing" [19]. One of the most challenging privacy issues in this context is to reconcile this continuous flow of data with privacy protection. One possible option to improve the situation when data has to be disclosed (or when it is practically impossible to object to its disclosure) is to enhance the obligations of the controllers and enforce more stringent rules on the use of personal data. We have followed this approach, considering both

- technical means to define and enforce obligations and
- possible evolutions of data protection regulations to avoid discriminations based on the use of personal data.

Technical means: specification and a posteriori verification of obligations

A major challenge for the formalization of privacy policies is the integration of deontic and temporal operators. Deontic operators are required because privacy policies are typically expressed in terms of obligations and interdictions. Temporal operators are necessary because obligations and interdictions usually come with deadlines: for example, the controller must inform the data subject before forwarding his data to a third party

or must delete the data within a given period of time. On the theoretical side, the limitations of Standard Deontic Logic (SDL) have constantly been pointed out, almost since its introduction. However, no other unified mathematical formalization of this logic has been proposed so far. Instead, many specialized logics have been put forward, each aimed at addressing one particular issue. To adddress this challenge, we have proposed a language called FLAVOR (Formal Language for A posteriori Verification Of legal Rules) for the expression of privacy policies and, more generally, obligations to be fulfilled by organizations. Indeed, organizations have to comply with a growing number of legal rules stemming from law, regulations, corporate policies or contractual agreements. Generally speaking, the actions to be monitored can be checked either *a priori* or *a posteriori*. *A priori* checks are stronger in the sense that they make it possible to ensure that no breach will occur. However, they are too constraining, if not inapplicable, in many situations. Even when they could be implemented, *a priori* checks are not desirable in situations in which it could be legitimate to bypass the rules. For instance, it is necessary to provide emergency procedures to access personal health records when human lifes are at stake, even if the medical practitioner on duty does not have sufficient permissions. The essential features provided by FLAVOR are the possibility to express "contrary to duty" obligations (substitute obligations to be fulfilled in case of breach of the primary obligation), obligations with deadlines and contextual obligations. We have defined a strength ordering between obligations and illustrated the language with typical privacy policy rules [10]. We have also considered the delegation of obligations between actors in [8] and studied the impact of delegation on different types of responsabilities (causal, functional, legal).

Legal means: privacy and non discrimination

In order to address the new threats to individual rights that are made possible by the progess of information technologies, we have proposed to distinguish two very different types of data collection [9]:

1. The collection of data as part of formal procedures with clearly identified parties or in the course of clearly identified events, recognized as such by the subjects (e.g. when submitting a file, filling a questionnaire, using a smart card or providing one's fingerprint to get access to a building).
2. The apparently insignificant and almost continuous collection of data that will become more and more common in the digital society (digital audit trails, audio and video recordings, etc.). This collection may be more or less perceived or suspected by the subject or remain completely invisible and unsuspected. Another worrying phenomenon is the automatic generation of new knowledge using data mining and knowledge inference techniques. In this kind of situation, the subject may ignore not only the process but also the generated knowledge itself, even if this knowledge is about him and could be used to take actions affecting him (e.g. not offering him a job or an insurance contract or adjusting the price of a service up to the level he would be prepared to pay).

The regulations on personal data protection were originally designed to address the first type of situation. Efforts are made to adapt them to the complex issues raised by the second type of data collection but they tend to be increasingly ineffective in these situations. The main cause of this ineffectiveness is their underlying philosophy of *a priori* and procedural controls. Starting from this observation, we have argued that a possible option is to strengthen *a posteriori* controls on the use of personal data and to ensure that the victims of data misuses can get compensations which are significant enough to represent a deterrence for data controllers. We have also argued that the consequences of such misuses of personal data often take the form of unfair discriminations and this trend is likely to increase with the generalization of the use of profiles. For this reason, we advocate the establishment of stronger connections between anti-discrimination and data protection laws, in particular to ensure that any data processing resulting in unfair differences of treatments between individuals is prohibited and is subject to effective compensations and sanctions [9].

6. Contracts and Grants with Industry

6.1. Contracts with Industry

The European project FI-WARE involves various industrial actors in the areas of security and internet services. The main interactions of LICIT within the project are with Nokia Siemens, SAP and Thales.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. Lise (ANR)

The LISE [5] project started in 2008 and is funded by the ANR SESUR programme. LISE is coordinated by LICIT and involves the AMAZONES and POP ART INRIA project-teams, the Law Faculty of Versailles Saint-Quentin, the Law Faculty of Caen, VERIMAG and SUPELEC.

One of the motivations of the LISE project is the fact that, as observed by several authors, software quality and patterns of security frauds are directly related to legal liability patterns. But the precise definition of the expected functionalities of software systems is quite a challenge, not to mention the use of such definition as a basis for a liability agreement. Taking up this challenge was precisely the objective of LISE. To achieve this goal, the project has studied liability issues both from the legal and the technical points of view with the aim to put forward methods (1) to define liability in a precise and unambiguous way and (2) to establish liability in case of disagreement [5], [12], [11].

7.1.2. Fluor (ANR)

The FLUOR [6] project started in 2008 and is funded by the ANR SESUR programme. FLUOR is coordinated by ENSTB and involves the CNRS (IODE), INRIA (LICIT), the LIUPPA (University of Pau), SWID and the University of Polynésie Française.

The context of the FLUOR project is the protection of corporate documents circulating within companies. The main objectives of the project are (1) to unify information flow models and usage control models and (2) to analyse the legal issues raised by the use of these documents. Emphasis is put by LICIT on the specification of obligations within organizations [10].

7.2. European Initiatives

7.2.1. FP7 Projet

7.2.1.1. FI-WARE

Title: Future Internet Ware.

Type: COOPERATION (ICT).

Defi: PPP FI: Technology Foundation: Future Internet Core Platform.

Instrument: Integrated Project (IP).

Duration: May 2011 - April 2014.

Coordinator: Telefonica. (Spain)

Others partners: SAP (Germany), IBM (Israel, Switzerland), Thales Communications (France), Telecom Italia (Italy), France Telecom (France), Nokia Siemens Networks (Germany, Hungary, Finland), Deutsche Telekom (Germany), Technicolor (France), Ericsson (Sweden), Atos Origin (Spain), Ingeneria Informatica (Italy), Alcatel-Lucent (Italy, Germany), Siemens (Germany), Intel (Ireland), NEC (United Kingdom), Fraunhofer Institute (Germany), University of Madrid (Spain), University of Duisburg (Germany), University of Roma La Sapienza (Italy), University of Surrey (United Kingdom).

See also: http://www.fi-ware.eu/.

[5] http://licit.inrialpes.fr/lise/
[6] http://fluor.no-ip.fr/

Abstract: The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. The project unites major European industrial actors in an unique effort never seen before. The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support emerging Future Internet (FI) services in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery - building a true foundation for the Future Internet.

7.3. International Initiatives

7.3.1. Visits of International Scientists

Visiting scientist (one month): Gerardo Schneider from the university of Chalmers (Gothenburg, Sweden).

8. Dissemination

8.1. Animation of the scientific community

As part of the networking activities put forward in Section 2.1, LICIT has organized or co-organized the following events:

- Multidisciplinary conference on digital evidence (Palais de Justice de Paris, December 2011) [7]. The other organizer was ADIJ (Association pour le Développement de l'Informatique Juridique). This conference was organized in the context of the LISE project.
- Multidisciplinary workshop on legal and technical aspects of causality (ENSCP Paris, December 2011) [8]. This open workshop was organized in the context of the LISE project.
- Annual Conference on Computers, Privacy and Data Protection CPDP 2011 (Brussels, January 2011) and panel on "behavioural targeting" [9]. CPDP, which is now established as the main privacy conference in Europe, attracts every year a wider and more multidisciplinary audience (more than 300 participants in 2011). The other organizers of CPDP are the Free University of Brussels (VUB), the University of Tilburg, the University of Namur and the Fraunhaufer Institute.

Daniel Le Métayer was a member of the PhD committee of Mario Alvim (École Polytechnique, Formal approaches to information hiding: an analysis of interactive systems, statistical disclosure control, and refinement of specifications), of the committee of the CNIL PhD award [10] and the scientific committees of :

- The Annual Conference on Computers, Privacy and Data Protection (CPDP 2011).
- The National Workshop on Privacy Protection (APVP 2011).

[7] http://licit.inrialpes.fr/lise/
[8] http://licit.inrialpes.fr/lise/
[9] http://www.cpdpconferences.org
[10] http://www.cnil.fr/la-cnil/actualite/prix-de-these/

Daniel Le Métayer gave the following invited talks:

- Conference on Software Engineering and Formal Methods (Montevideo, November 2011): *Formal methods as a link between software code and legal rules*.
- University of Laval (Québec, October 2011): *Privacy by design: towards a systematic approach.*
- INRIA-CELAR Seminars “Formal methods and security" (Rennes, July 2011): *Méthodes formelles et protection de la vie privée (“Formal methods and privacy protection").*
- Colloque “Electronique ambiante", Parlement du Futur, (Assemblée Nationale, Paris, May 2011): *Des outils pour mieux protéger la vie privée (“Privacy enhancing tools").*
- Exhibition “Tous connectés" on pervasive computing (CCSTI, Grenoble, February 2011): *Des outils pour mieux protéger la vie privée (“Privacy enhancing tools").*
- LIRIS Seminars (Lyon, February 2011): *Méthodes formelles et droit (“Formal methods and regulations").*
- TURBINE workshop on Privacy in ITS Applications (Brussels, January 2011): *Privacy by design: towards a systematic approach.*

8.2. Teaching

PhD in progress : Eduardo Mazza, Specification of liability issues in software engineering, November 2008, Daniel Le Métayer

PhD in progress : Thibaud Antignac, A systematic approach to privacy by design, September 2011, Daniel Le Métayer

9. Bibliography

Major publications by the team in recent years

[1] D. LE MÉTAYER (editor). *Les technologies au service des droits, opportunités, défis, limites*, Bruylant, Cahiers du CRID No 32, 2010.

[2] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRENOT, V. VIET TRIEM TONG, N. CRAIPEAU, R. HARDOUIN. *Liability in software engineering: overview of the LISE approach and application on a case study*, in "International Conference on Software Engineering, ICSE’2010", ACM/IEEE, 2010, p. 135-144.

[3] D. LE MÉTAYER, E. MAZZA, M.-L. POTET. *Designing log architectures for legal evidence*, in "8th International Conference on Software Engineering and Formal Methods, SEFM’2010", IEEE, 2010, p. 156-165.

[4] D. LE MÉTAYER, S. MONTELEONE. *Automated consent through privacy agents : legal requirements and technical architecture*, in "The Computer Law and Security Review, Elsevier", 2009, vol. 25(2).

Publications of the year

Articles in International Peer-Reviewed Journal

[5] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRENOT, V. VIET TRIEM TONG, N. CRAIPEAU, R. HARDOUIN. *Liability issues in software engineering. The use of formal methods to reduce legal uncertainties*, in "Communications of the ACM", 2011, vol. 54, 4, p. 99-106.

Articles in National Peer-Reviewed Journal

[6] D. LE MÉTAYER. *Responsabilités du fait des logiciels: prendre en compte les exigences juridiques dès la phase de conception pour faciliter le règlement ultérieur des différends*, in "Revue Lamy Droit de l'Immatériel", 2012, to appear.

Invited Conferences

[7] D. LE MÉTAYER. *Formal methods as a link between software code and legal rules*, in "9th International Conference on Software Engineering and Formal Methods, SEFM'2011", G. BARTHE, A. PARDO, G. SCHNEIDER (editors), Lecture Notes in Computer Science, Springer, 2011, vol. 7041, p. 13-18.

International Conferences with Proceedings

[8] M. B. GHORBEL-TALBI, F. CUPPENS, N. CUPPENS-BOULAHIA, D. LE MÉTAYER, G. PIOLLE. *Delegation of Obligations and Responsibility*, in "Proceedings of the IFIP SEC 2011 Conference - Future Challenges in Security and Privacy for Academia and Industry", IFIP publisher Springer Science and Business Media, 2011, p. 197-209.

[9] D. LE MÉTAYER, J. LE CLAINCHE. *From the protection of data to the protection of individuals: extending the application of non discrimination principles*, in "European Data Protection: In Good Health ?", S. GUTWIRTH, Y. POULLET, P. DE HERT (editors), Springer Verlag, 2012, to appear.

[10] R. THION, D. LE MÉTAYER. *FLAVOR: a formal language for a posteriori verification of legal rules*, in "Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks", IEEE, 2011, p. 1-8.

National Conferences with Proceeding

[11] L. ASTEFANOAEI, G. GOESSLER, D. LE MÉTAYER, E. MAZZA, M.-L. POTET, V. VIET TRIEM TONG. *Apport des méthodes formelles pour l'exploitation de logs informatiques dans un contexte contractuel*, in "Proceedings of the Conference Approches Formelles dans l'Assistance au Développement de Logiciels", AFADL, 2012, to appear.

[12] S. STEER, N. CRAIPEAU, D. LE MÉTAYER, M. MAAREK, M.-L. POTET, V. VIET TRIEM TONG. *Définition des responsabilités pour les dysfonctionnements de logiciels: cadre contractuel et outils de mise en oeuvre*, in "Proceedings of the Conference Droit, sciences et techniques, quelles responsabilités ?", Litec, LexisNexis, 2011, p. 199-216.

References in notes

[13] L. L. FULLER. *The morality of law*, Yale University Press, 1964.

[14] D. LE MÉTAYER, A. ROUVROY. *STIC et droit : défis, conflits et complémentarités*, in "Interstices", November 2008, http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites.

[15] L. LESSIG. *The future of ideas: the fate of the commons in a connected world*, Random House, 2001.

[16] L. LESSIG. *Code and other laws of cyberspace, Version 2.0*, Basic Books, 2007.

[17] Y. POULLET. *The Directive 95/46/EC: ten years after*, in "Computer Law and Security Report", 2006, vol. 22, p. 206–217.

[18] J. REIDENBERG. *Lex informatica: the formulation of information policy rules through technology*, in "Texas Law Review", 1998, vol. 76, n^{o} 3.

[19] A. ROUVROY. *Privacy, data protection and the unprecedented challenges of ambient intelligence*, in "Studies in Ethics, Law and Technology, Berkley Electronic Press", 2008.