Canadian Journal of Law and Technology

Volume 7
Number 1 *1 & 2*

Article 2

1-1-2010

Groundwork for Assessing the Legal Risks of Cyberjustice

François Senécal

Karim Benyekhlef

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

Recommended Citation

Senécal, François and Benyekhlef, Karim (2010) "Groundwork for Assessing the Legal Risks of Cyberjustice," *Canadian Journal of Law and Technology*: Vol. 7 : No. 1 , Article 2.
Available at: https://digitalcommons.schulichlaw.dal.ca/cjlt/vol7/iss1/2

This Article is brought to you for free and open access by the Journals at Schulich Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Scholars. For more information, please contact hannah.steeves@dal.ca.

Groundwork for Assessing the Legal Risks of Cyberjustice

François Senécal & Karim Benyekhlef*

INTRODUCTION

The legal systems of Western countries are the results of centuries of development, adaptation and difficult balancing of competing values. The interface through which individuals gain access to justice used to be based on oral procedures, then on writings, but is now at the dawn of a new medium. Criminal and civil justice proceedings are still strongly attached to paper and the physical presence of parties. Yet, according to some, "courts cannot continue to be 'paper islands' in an 'electronic ocean.'"[1] Today, as information and communications technology is spreading through legal systems, the idiosyncrasies of the latter are being exacerbated by new emerging issues. The electronic medium, with its inherent characteristics and its potential, is shaking the relative immutability of legal systems.

This phenomenon is not new. An example of the impact that a change in medium can have is the introduction of the printing press, which in the sixteenth century spread into virtually every area of public life. From a legal history point of view, this contributed significantly to the development of the notion of legal precedent. While manuscripts were unique (in particular owing to the mistakes of copyists) and limited in number, the printing press made it possible to produce multiple copies of a document and, at the same time, ensure that they were identical. "Printing, unlike writing, allowed a society to build on the past with a confidence that each step was being made on a firm foundation."[2] Until then, previous decisions were only images of the law, not the law itself.[3] By the eighteenth century, trust in the printing press was taken for granted, and the precedent doctrine, as we know it today, could be consolidated. In 1765, Lord Camden asserted, "[i]f it is law, it will

---

* Respectively, Master's student and Director, Centre de recherche en droit public, Faculté de droit Université de Montréal. The authors wish to thank the Social Science and Humanities Research Council of Canada (SSHRC) for financing the research and writing of this text, Nicolas W. Vermeys for his insightful comments, and Julia Rys for her thorough proof-reading.

1 Melbourne, Australian Institute for Judicial Administration, "Technology for Justice — 2002 Report" by Jeff Leeuwenburg & Anne Wallace (2003) at 11, online: The Australasian Institute of Judicial Administration <http://www.aija.org.au/tech3/report.pdf>.

2 M. Ethan Katsh, *The Electronic Media and the Transformation of Law* (New York: Oxford University Press, 1989) at 34.

3 *Ibid.* at 37.

be found in our books. If it is not to be found there, it is not law."[4] The printed medium thus confers the stability needed for the development of law by precedent.

The printed medium also led to an improved organization of public law: "The systematic arrangement of titles; the tables which followed strict alphabetical order; the indexes and cross-references to accurately numbered paragraphs all show how new tools available to printers helped to bring more order and method into a significant body of public law."[5] The passage from an oral to a printed culture made sources of law available and, through systemization, brought method to law's internal structure. Consequently, the relevance of "immemorial custom" collapsed.[6] These two examples illustrate that law, far from developing in a vacuum, is not independent of the dominant medium of the society that it regulates. This observation leads us to inquire into the effect of the constantly growing use of electronic media and information technology on state legal systems.

It is clear that the use of information technology is quickly becoming a necessity for the justice system. In civil cases, delays and costs are causing individuals to abandon the courts, and cases that make it to trial are of ever-increasing complexity.[7] Moreover, public security is weakened by the inefficient and cumbersome conditions by which criminal justice information circulates among the various stakeholders, such as the police, prosecutors, the courts, penitentiaries and parole boards, to name only a few. It becomes apparent that information technology has much to offer individuals involved in court cases and the justice system as a whole.

We have every reason to think that this change in medium will affect law, in general, and rights, in particular. At the same time, legal systems can clearly be improved by the use of new information and communication technology. These two observations call for reflection on the implications of computerizing and networking the justice system, where the requirements of legal certainty — demanding a prospective study of the risks entailed by the change — will be met. It will also make it possible to guide the way in which computer potential is used in legal proceedings and justice information. To that end, we will sketch out the broad lines of a method for assessing legal and judicial risks flowing from the implementation of cyberjustice systems.

---

4 *Entick v. Carrington*, [1558-1774] All E.R. Rep. 41, 95 ER 807, (1765) 19 St. Tr. 1030, [1765] EWHC KB J98 as paraphrased in Katsh; *Ibid.* at 39.

5 Elizabeth L. Eisenstein, *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early Modern Europe* (New York: Cambridge University Press, 1979) at 105.

6 See generally M.T. Clanchy, *From Memory to Written Record: England 1066-1307*, 2nd ed. (Cambridge, Mass.: Oxford, Blackwell, 1993).

7 Justice François Rolland, "Access to Justice: 3 Years After the Reform of the Code of Civil Procedure" (Address given to the "Into the Future — The Agenda for Civil Justice Reform", Montreal, 1 May 2006) at 7–10, online: Canadian Forum on Civil Justice <http://cfcj-fcjc.org/docs/2006/rolland-en.pdf>.

I. A WORKING DEFINITION OF CYBERJUSTICE

First, we have to point out that there is some ambiguity in the terminology relating to the notion of cyberjustice. This short section will situate the problem and establish a working definition.

A cyberjustice system has to be considered the conjunction of different modules designed to achieve a global purpose. For example, electronic filing, in which a document is sent by telecommunications to be filed in the registry of a court, is only one module of a broader set. The features of cyberjustice systems can be very different depending on the interface (communication channel and markup language) and extent of the services offered. If electronic filing is accompanied by automatic service to the opposing party, it is clear that the organizational and conceptual separation between filing and service is eliminated. This means that risk assessment should not take for granted a system's denomination, but rather the informational and functional characteristics of its modules.

Electronic filing is a component of judicial and other case management systems. The purpose of such systems is to manage a case throughout its lifecycle, from filing to final settlement. The networking and automation of judicial procedures are therefore at the very core of this process. Their functions have to be viewed from the perspective of managing procedures and the interactions of parties to a case. In this respect, there can be different modules for functionalities such as:

> . . . remote appearance, study of petitions and other preliminary and interlocutory applications without the physical presence of the parties; electronic notification or service of proceedings and even some decisions (proceedings management); management of court records, dockets, hearings, rooms, schedules, digital recordings and internal resources; and execution of financial aspects of court cases (e.g., management of deposits, bail, power of attorney).[8]

The Australian *Casetrack* system[9] is an example of a case management system. Another example is British Columbia's *JUSTIN* system,[10] which is used in criminal law and available only to the Crown.

These case management systems and their many functionalities mainly concern the computerization of court procedures. They are part of a larger set, namely that of integrated justice information systems, which is distinguished by strong in-

---

8 Karim Benyekhlef & Fabien Gélinas, *Le règlement en ligne des conflits — Enjeux de la cyberjustice* (Paris: Romillat, 2003) at 37 [translated by authors.].

9 Federal Court of Australia, The *eCourt Strategy* (2007), online: Federal Court of Australia <http://www.fedcourt.gov.au/ecourt/ecourt_strategy.html>.

10 British Columbia Ministry of Attorney General, *JUSTIN* (2007), online: Attorney General — Province of British Columbia <http://www.ag.gov.bc.ca/justin/>.

ter-institutionality. The definition proposed by the National Criminal Justice Association in the United States is clear on this point:

> The term "integrated justice systems" encompasses *interagency*, *interdisciplinary*, and *intergovernmental* information systems that access, collect, use, and disseminate critical information at key decision points throughout the justice process, including building or enhancing capacities to automatically query regional statewide and national databases and to report key transactions regarding people and cases to local, regional, statewide, and national systems. Generally, the term is employed in describing justice information systems that eliminate duplicate data entry, provide access to information that is not otherwise available, and ensure the timely sharing of critical information.[11]

This definition highlights the primarily informational nature of justice processes and suggests that cyberjustice could be implemented across a very broad range of judicial activities. At this point, we can suggest that the term "cyberjustice" refers both to the integration of information and communication technologies into dispute resolution processes and to the networking of all stakeholders in the informational chain for judicial cases.

In Canada, the federal government is establishing the National Integrated Interagency Information (N-III) system, which will "[enable] broader information sharing and integrated investigations among Canada's law enforcement and justice communities."[12] It is composed of the Police Information Portal (PIP), which makes it possible to search police information systems, and the Integrated Query Tool (IQT), which makes information exchanges possible, particularly between the Royal Canadian Mounted Police, Canada Border Services Agency and Canada Firearms Centre.[13]

It should be noted that Canada's federal nature entails specific requirements and problems relating to the division of jurisdiction with respect to law. Thus, administration of justice is under provincial jurisdiction, but many federal institutions are involved in justice processes.

The scope of cyberjustice systems developed in different jurisdictions varies greatly, as do the methods and technologies employed. Therefore, study of these

---

11 National Criminal Justice Association, *Justice Information Privacy Guidelines — Developing, Drafting and Assessing Privacy Policy for Justice Information Systems* (2002) at 16, online: National Criminal Justice Association <http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf>, cited in Benyekhlef & Gélinas, *supra* note 8 at 35-36.

12 Royal Canadian Mounted Police, "Departmental Performance Report for the Period Ending March 31, 2006" (2006) at 35, online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/dpr-rmr/0506/RCMP-GRC/rcmp-grc_eng.pdf>.

13 *Ibid.* at 35, 112; Standing Senate Committee on National Security and Defence, "An Update of Security Problems in Search of Solutions — Border Crossings" (2007) at 82, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/defe-e/rep-e/rep10mar07-e.pdf>.

systems and assessment of the associated risks have to take the systems' specific features into account so as to avoid terminological traps and, above all, establish a method applicable to cyberjustice systems no matter how different they are from one another.

The concept of an "information lifecycle" is central to the analysis of information management issues. In a report[14] on assessing risks to privacy entailed by Quebec's Integrated Information Justice System (IJIS), the *Centre de recherche en droit public* at the Université de Montréal developed an analytical approach to the study of information environments based on the entire information lifecycle: "from its creation, if applicable, its collection, its management, its flow, its use, its archiving and its destruction."[15] Thus, the first step is to "identify the characteristics of these [informational] environments, which information pools and flows they imply or authorize, what they facilitate, authorize or prevent us from doing."[16] In other words, it is to identify the function of each module of the cyberjustice system.

The basic components of informational environments are information pools, flows and processes. Information pools are sources such as databases and electronic files. Information flows are the routes that information takes between different pools and stakeholders, for example, publication of court decisions, electronic filing and networking of police information and civil registers. Finally, information processes are the use that is made of information, such as database queries, cross referencing, analysis or anonymization.

Based on the system description, the second step was the identification of areas of risk to privacy, during the information's entire lifecycle within the environment and according to the type of information.[17] This systematic, structured and deductive approach has the merit of avoiding pre-supposition of risks and catastrophic scenarios, thereby making it possible to identify features that could cause problems and enabling risk management solutions to be found and implemented.

According to the proposed definition, a cyberjustice system is an informational environment, composed of various modules and functions, where the information lifecycle is revealed by the basic components of the environment. As such, it enables the approach described above.

---

14 Karim Benyekhlef & Pierre Trudel, *Analyse des risques pour la protection des renseignements personnels dans le Système intégré d'information de justice (SIIJ)* (Montréal: Centre de recherche en droit public, 2003) [unpublished].

15 Pierre Trudel, *Droit, régulation et protection de la vie privée dans le e-gouvernement* (Montréal: Centre de recherche en droit public, 2008) at 116 [translated by authors].

16 *Ibid.*

17 *Ibid.* at 117.

II. THE NEED FOR A COMPREHENSIVE RISK ASSESSMENT THEORY FOR CYBERJUSTICE

Use of information and communication technology in the legal field is growing and rendering a return to past methods as inconceivable. Proof of this can be seen in the expansion of Online Dispute Resolution (ODR) services in e-business and especially in the interest in cyberjustice in almost every industrialized country.[18] Indeed, the same problems are arising everywhere: unreasonable waiting times, skyrocketing costs and the increased complexity of cases. However, successful implementation of cyberjustice systems depends in part on the ability to develop analyses that clarify the legal framework of such systems. Such analyses have to take into account constitutional and legal imperatives and the reasons behind the proposed changes. In this respect, much remains to be done.

The primary difficulty that limits such analyses and prevents a definition of the legal framework for cyberjustice systems is the lack of a theory for assessing legal and judicial risks. Two major consequences flow from this. First, research on these new aspects of law is disorganized. Very little work has been done on the effects of cyberjustice on the justice system. In fact, what has been done mainly concerns privacy protection. Second, research has been fragmented. Since different jurisdictions are working on cyberjustice systems in isolation, it is impossible to perform a systematic general analysis of legal risks. Thus, we need a framework for organizing this field of research, which, at the moment, appears to be in a state of limbo. The central importance of legal systems in our societies makes this a crucial issue.

The first step toward eliminating the lack of organization is the clarification of cyberjustice terminology. In other words, we need to better define this new reality in order to better understand it. For the purposes of this article, a working definition has been proposed. This should facilitate comparisons among different systems. Based on the definition, the second step, presented below, is to develop a methodology for assessing the legal risks of cyberjustice systems.

III. FIRST STEPS TOWARDS A METHODOLOGY FOR RISK ASSESSMENT

> *[S]he might change at times the empty treasures*
> *From race to race, from one blood to another,*
> *Beyond resistance of all human wisdom.*
> *Therefore one people triumphs, and another*
> *Languishes, in pursuance of her judgment,*
> *Which hidden is, as in the grass a serpent.*
> *Your knowledge has no counterstand against her;*

18 As early as in 2001, the Research Institute on Judicial Systems of the University of Bologna organized a seminar and gathered status reports on the use of IT in the judicial from over 20 countries, mainly European: see Francesco Contini & Marco Fabri, eds., *Judicial Electronic Data Interchange in Europe* (Bologna: Lo Scarabeo, 2003).

She makes provision, judges, and pursues
Her governance, as theirs the other gods.

Dante, *The Divine Comedy — Hell*, Canto VII
(Henry Wadsworth Longfellow's translation)

In the passage above, Virgil describes the goddess Fortuna to Dante. The course of events is determined by the goddess of fortune and her wheel. Humanity is discharged of control over its destiny: chance is almighty. In such a mythological view of the world, causes of events are externalized, if indeed we can really speak of "causes." In the present section, we will examine the idea that the architecture of artefacts convey values and therefore cannot help but generate risks. This will be followed by a discussion of the notion of risk; on one hand, establishing the context in which legal risk will be defined and, on the other hand, proposing a theory for assessing such risks.

(a) "Do Artefacts Have Politics?"[19]

Ulrich Beck suggests that modern post-industrial societies have internalized risk. The new modernity is reflexive: society has to respond to problems caused by its own activity. Human activity generates "latent induced effects" that have to be identified and controlled. Society no longer develops according to a system of distribution of wealth but according to a division of risk. The central issue of the new paradigm is: "How can the risks and hazards systematically produced as part of modernization be prevented, minimized[,] limited and distributed away so that they neither hamper the modernization process nor exceed the limits of that which is 'tolerable'?"[20] The study of legal risks engendered by the implementation of cyberjustice systems must occur prior to such effects: its purpose is to anticipate them with a view to security and maintenance of social peace.

Some authors acknowledge that artefacts, i.e. human constructions, can convey values and even have normative consequences.[21] For instance, in the 1970s, it was recognized that some urban environments excluded disabled people from public life owing to the absence of access ramps. Once the problem was acknowledged, changes were made and this had an impact on how the right to equality was respected.[22] Langdon Winner concludes that "[t]he issues that divide or unite people in society are settled not only in the institutions and practices of politics proper,

19 Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: University of Chicago Press, 1986) at 19.

20 Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE Publications, 1992) at 19.

21 Lawrence Lessig, *Code v. 2.0* (New-York: Basic Books, 2006); Joel Reidenberg, "Lex Iinformatica: The Formulation of Information Policy Rules through Technology" (1998) 76 Texas Law Review 553; Winner, *supra* note 19.

22 Winner, *supra* note 19 at 25.

but also, and less obviously, in tangible arrangements of steel and concrete, wires and semiconductors, nuts and bolts."[23] In the case at hand, making the necessary observations can be done as part of a process: if it is integrated into the development stage, assessment of the legal risks of a cyberjustice system is much more relevant to decision-makers and individuals.

However, it is possible to take thought on the effects of cyberjustice a step further. The crucial issue is whether cyberjustice is "merely a new method for handling [an] age-old task" or, in fact, something that changes the social fabric and adds new facets to human activity.[24] Recognition of such profound changes does not, however, belong uniquely to the field of law.

(b) Risk and Risk Management

Unlike fortune, risk entails that stakeholders have a certain degree of choice of whether to expose themselves to it. Semantically, the notion of risk overlaps with those of chance, randomness and danger, but, by definition, implies the conditions under which it is acceptable: "[a] willingness to balance relative costs and benefits is inherent in the very adoption of the concept of "risk" to describe one's situation."[25] This "transactional" aspect of "risk" is not found in the notions of danger or peril. While the notion of danger is that of an observation about an objective situation, the notion of risk is ambivalent and entails the question of whether it is acceptable to the stakeholder:[26] "how safe is safe enough?"[27] It is "closely . . . linked to the sense of voluntary undertaking."[28] Faced with a given action, "[t]he alternative is not between, on one hand, risk and, on the other hand, absence of risk, but indeed between acceptable and unacceptable risk."[29]

Risks combine prediction and damage potential: they "signify a future which is to be prevented."[30] Motivation for action is, therefore, to avoid, attenuate and prevent.[31] This is the focus of risk management, which is based on the negotiable nature of risk.

Exposure to risk "is defined as a function of the probability of a negative outcome and the importance of the loss due to the occurrence of this outcome."[32] This

---

23 *Ibid.* at 29.

24 *Ibid.* at 13.

25 *Ibid.* at 145.

26 Christine Noiville, *Du bon gouvernement des risques* (Paris: Presses Universitaires de France, 2003) at 2 [translated by authors].

27 Winner, *supra* note 19 at 138.

28 *Ibid.* at 145.

29 Noiville, *supra* note 26 at 3.

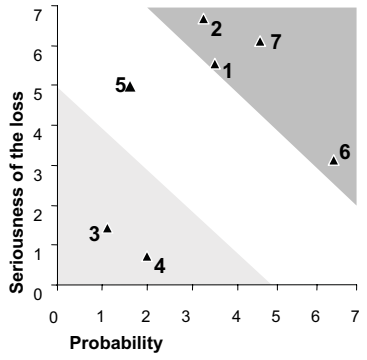
30 Beck, *supra* note 20 at 33.

31 *Ibid.* at 34.

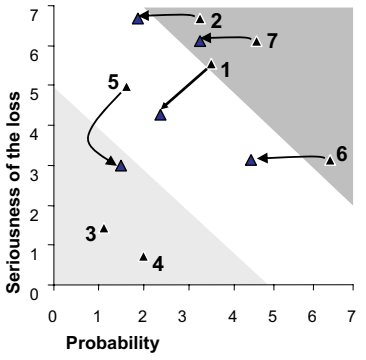
32 Benoit A. Aubert, Michel Patry & Suzanne Rivard, "A Framework for Information Technology Outsourcing Risk Management" (2005) 36:4 ACM SIGMIS Database 9 at 11. The mathematical formula is "$RE = \Sigma_i P(UO_i) * L(UO_i)$, where $P(UO_i)$ is the

already presupposes the identification of different undesirable outcomes, which could include cost over-runs, delays, poor quality, dissatisfaction, etc. Each undesirable outcome can then be represented on a chart with the axes of probability and seriousness of the potential loss. The least serious and least likely risks, in other words, those that are the lowest, are visually separated from the more serious or more probable risks. Taking measures to deal with the latter will tend to shift them from a zone in which they are not acceptable into one where they are in terms of probability or seriousness. This is illustrated in the graphs below.

Graph 1: Exposure to risk



Graph 2: Effect of risk management



Source: Suzanne Rivard, "Quand la recherche devient pratique: le cas de la gestion du risque de projets de technologies de l'information" (Presentation given at the Conférence Prix Gérard-Parizeau, Montréal, 19 April 2007) [unpublished; our translation]. Reprinted with permission.

While the first graph illustrates exposure to risk, the arrows on the second represent the effect of risk management on risk acceptability: the less probable or less serious the risk, the more acceptable it is. For example, networking police databases (i.e. making information easier to access) can affect the principles of presumption of innocence or right to privacy if they are consulted systematically or blindly (e.g. by going on a "fishing expedition"). However, by providing a framework for their use, such as by requiring a warrant based on reasonable and probable cause to believe there is a link between an individual and a crime, and by logging databases queries, the risk is brought down into a more acceptable zone. Thus, risk management makes it possible to achieve the desired results while minimizing undesirable side effects. In the above case, in which the objective is public security and the means are better access to information, there could be harmful consequences for fundamental rights if there were no control measures. Conversely,

---

probability of an undesirable outcome *i*, and $L(UO_i)$ the loss due to the undesirable outcome *i*", Σ being the symbol of summation.

some measures could even better protect these rights. However, the efficiency of risk management is based on adequate identification of risks and, especially, of the factors that contribute to them.

(c) Defining Legal Risk

The way risk is defined differs from one field to the next: "[e]ach field addresses risk in a fashion relevant to its object of analysis, hence, adopts a particular perspective."[33] In insurance, risk is the measure of the predicted loss; in finance, it is equated with the variability and volatility of the yield of a portfolio; and in some other fields, like medicine, risk is seen as a function of probability where the focus is oriented towards odds of occurence rather than consequences.[34]

Therefore, we have to identify the object of legal risk. In the above examples, the object of the risk is an element (dependent variable) that is likely to be subjected to the effects of variations of other elements (independent variables): the insurance company's measure of a loss is a function of a number of factors, such as the value of a building and its use. In our case, we aim to assess the consequences of a change in the media on which justice processes are based and of changes in justice information pools, flows and processes: these are the independent variables. As our hypothesis poses that these changes will affect law and rights, we suggest that the object of legal risks is the different basic tenets of the justice system, which are likely to suffer variations and effects related to those changes. By basic tenets, we mean basic legal rights, the values embodied by the justice system and the various principles on which it is based. For example, consider the legal guarantees contained in sections 7 to 14 of the *Canadian Charter of Rights and Freedoms*, in particular the principles of fundamental justice such as the right to a fair and equitable trial, judicial independence, protection against unreasonable search or seizure, and access to justice. Some values and other basic tenets can be more difficult to identify. Far from being set out in constitutional provisions, they can be embodied in custom and tradition. Symbolism and ritual, which play a big role in the justice system, are also affected by the change in medium. Their purpose is intimately related to public trust in courts and tribunals, and to the authority of such institutions with respect to ascertaining facts and law. Major procedural elements can also be affected by cyberjustice. For instance, video recordings of testimony could challenge the primary reason for appeal court deference to lower courts with respect to examination of evidence, namely, the fact that appeal court judges do not attend lower court hearings. Moreover, the availability of such images, rather than mere transcripts, to the media could have a strong impact on some witnesses.

Legal risk itself still has to be defined. As we saw above, for Winner, Lawrence Lessig and Joel Reidenberg, artefacts can embody values, have social impacts and even normative effects. For Beck, risk is a by-product of human activity. In both cases, undesirable outcomes may occur. Risk, in this conception, "is equated

33 *Ibid.* at 10.

34 *Ibid.*

to a possible negative event. '[An event] that, if [it] occur[s], represent[s] a material threat to an entity's fortune.'"[35] Given the context of cyberjustice projects and the object of legal risk, legal risk is close to the notion of threat, but may lack its external character. Indeed, a cyberjustice project being an entirely artificial environment upon which control can be exercised and liability be attributed, risks will also be influenced by vulnerabilities, i.e. weaknesses of this environment.

Thus, the *object* of legal risk having been identified above as basic legal tenets, we suggest that legal risk should be defined as a possible harm to these basic tenets. Such harm could be, for example, a disruption of the balance among various rights (e.g. the principle of equality of arms, the right to public process and public availability of evidence vs. the right to privacy protection in an electronic world) or a loss of reference points owing to a change in medium (e.g. the impact on jury members of submissions enhanced by multimedia presentations). Unseen situations may also arise, some of which are obvious (e.g. screens blocking visual contact between the judge and parties, and document printing delays at the hearing),[36] others being more surreptitious (e.g. transformation of the investigative process by forces of law and order with access to many databases and cross-referencing tools).[37] Changes to judicial processes relating to information pools, flows and processes can affect values as well as their underlying purposes. Studying these risks will bring greater legal certainty to cyberjustice projects.

(d) Risk Assessment

The working definition of cyberjustice and the CRDP's privacy risk assessment scheme for the IJIS can be combined to produce a theory for assessing the legal risks of cyberjustice systems based on the analysis of informational components (pools, flows and processes) of system modules.

A similar approach has already been used. In the 1970s, the HAZOP (*Hazard Operability*) method for qualitative risk assessment was developed by Imperial Chemical Industries in the context of hydraulic system processes.[38] It is based on a "systematic, methodical examination of design documents that describe the facility — Deviations from the design value of key parameters are studied, using guide

---

35 *Ibid.*, citing M. Levin & M. Schneider, "Making the Distinction: Risk Management, Risk Exposure" (1997) 44:8 Risk Management 36 at 38.

36 John G. Farrell, "Electronic Case Files and Administrative Hearings: A View from the Bench" (2004) 24 Journal of the National Association of Administrative Law Judges 33.

37 Lawrence Lessig, "The Architecture of Privacy" (1998), online: Berkman Center for Internet and Society <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf> (Lessig argues that inefficient technologies "themselves constituted protection; they made it hard to search" and were, after the law, "a second line of defense against the invasion of prying eyes").

38 Hélène Denis, *Comprendre et gérer les risques sociotechnologiques majeurs* (Montréal: Éditions de l'École polytechnique de Montréal, 1998) at 28.

words to control the examination evaluation."[39] Each module of the system is the focus of questions formulated by matching various parameters, such as pressure, temperature and flow, with key terms, such as "no", "more", "less" and "partly." "The guide words are used to ensure that the questions, which are posed to test the integrity of each part of the design, will explore every conceivable way in which that design could deviate from the design intention."[40] Risks, defined here as "potential deviations", and their probable causes and consequences are identified. Corrective measures can be suggested to reduce risks so that, in the end, the system should be less risky — more *acceptable* — than it was at first.

The basic principle of this method of qualitative risk assessment is the questioning of a system's modules according to its environment's technical parameters and appropriate criteria — such as the guide words.

Such a method can be transposed into the context of cyberjustice systems. This is where the working definition of cyberjustice comes in. Modelling justice processes in cyberjustice systems (using synoptic tables, for instance) reveals their informational nature and identifies their technical features. Throughout its lifecycle, information is subject to pools, flows and processes. Schematizing processes makes it possible to visualize them and is an important risk assessment tool. It describes the architecture of the present system[41] or of one that is planned or in the process of being computerized.

Consequently, the modules of a cyberjustice system have to be broken down into components: information pools, flows and processes. This makes it possible to question cyberjustice modules in relation to the objects of legal risk, i.e., constitutional and legal requirements, values and principles (these can be assimilated to a set of guide words). Most such objects have already been identified, studied and discussed by the courts, although their criteria for assessment may not always be well established. Though cyberjustice will likely cause major changes, it will not cause a historical *tabula rasa*.

The following table contains a brief example of assessment of the legal risks of a module based on the use of digital recording technology in hearings:

---

39 R. M. Sherrod & W. F. Early, "Hazard and Operability Studies" in Harris R. Greenberg & Joseph J. Cramer, eds., *Risk Assessment and Risk Management for the Chemical Process Industry* (Mississauga: John Wiley & Sons, 1991) 101 at 101.

40 Netherlands Committee for Prevention of Disasters, *Methods for Determining and Processing Probabilities*, 2nd ed. (The Hague: Director General for Social Affairs and Employment, 1997) at 7.17, online: Ministry of Housing, Spatial Planning and the Environment <http://www.vrom.nl/Docs/milieu/200512_PGS4.pdf>.

41 For an example of modelization of current processes in Québec law, see Ministère de la justice du Québec, *Analyse préliminaire du Système intégré d'information de justice — Bilan de la situation actuelle* (2003) at annexes H-K, online: Ministère de la justice du Québec <http://www.justice.gouv.qc.ca/francais/publications/rapports/siij-analyse.htm>.

Table 1. Study of digital recording technology use in hearings

Technical features	Object of legal risk	Assessment criteria	Risk overview
Process — No anonymization process.	Privacy protection.	Privacy protection principles.	Low risk if not made available to the public.
Process — Possible use by electronic media.	Peace of mind of witnesses at the hearing.	To be determined.	To be determined.
Flow — Judges and the Crown have access through the court network.	Principle of equality of arms.	See doctrine and case law.	Unequal access to recordings could be inconsistent with the principle of equality of arms.
Flow — Recordings not available to the public, but transcripts are.	Right to public hearing and court proceedings (and corollaries, such as protection against perjury).	See doctrine and case law.	Since this situation is unchanged, the right to public proceedings might not be affected. But was the limitation imposed by the paper medium itself? In other words, is optimization possible?

Assessment of legal risks could be based on this kind of template, which covers both the technological features of cyberjustice systems and the basic tenets of legal systems — basic rights, values and other principles. These two choices can be justified. In the former case, modelling frees information pools, flows and processes from any reference to a medium, be it paper or electronic. In the latter case, the basic tenets are identified as the objects of legal risk, which we are trying to assess by looking at how they are affected by the medium change. Since the various constitutional and legal requirements and values have generally been studied in depth, they can be assessed using criteria that have already been developed by the courts and doctrine. This leaves open the possibility of rereading or challenging the criteria in the new environment, if necessary.

The quality of the final assessment will depend upon the information available about the technical features of the system, analysts' perspicacity or even imagination with respect to identifying the legal values at stake, and finally upon the legal analysis of the relationship between these values and technological features. Fric-

tion between the law and a technological feature will indicate a risk that ought to be considered and dealt with.

In accordance with CRDP's approach to identifying and assessing privacy risks, basic tenets and values are considered without reference to institutions established to embody and protect them in order to avoid confusion. Moreover, while the institutions that are the guardians of these values vary from one jurisdiction to the next, the values themselves are generally shared. Thus, the framework opens the way to studying how existing institutions can handle risks in accordance with their powers, expertise, resources and other specific features, such as flexibility and governance structure — in short, in accordance with their ability to manage changes to the justice system flowing from use of cyberjustice. The framework can also be used comparatively and across systems. Comparative law will be crucial for identifying and developing innovative solutions to new problems in all legal systems.[42]

IV. RESEARCH PERSPECTIVES

The purpose of this text is to suggest avenues for developing a method of assessing the legal risks of cyberjustice systems so as to better identify the effects of introducing information technology into justice systems. As necessary as such a study may be, it remains limited by its premises. On one hand, cyberjustice is not restricted to the simple transposition of paper-based procedures onto electronic media. On the other hand, and in a more fundamental way, the identified risks will have ramifications far beyond the field of law.

Just as the first printed books were intended to be perfect copies of handwritten works,[43] the first steps towards cyberjustice will naturally involve modelling and reproducing present paper processes using electronic media. This is only the beginning of use of information technology. They will not be used to their full potential in the first stage. However, this developmental stage is crucial because its success will have a major impact on the evolution of future cyberjustice systems. It is in the re-engineering of proceedings, supported by reasoning that takes the features of the new medium into account, that information technology's potential for improving the justice system will be fully unleashed. Civil procedure makes individual rights concrete: its rules are designed "to render effective the substantive law and to ensure that it is carried out."[44] Nevertheless, despite its fundamental importance, legal scholars tend to neglect procedure in favour of the law of evidence. Cyberjustice presents an opportunity to renew legal scholarship on the law of procedure.

Finally, the notion of justice is multifaceted and extends far beyond the law. Analysis of legal risks is only one aspect of a general study of the effects of

---

42 These requirements were set out in Fabien Gélinas, "Interopérabilité et normalisation des systèmes de cyberjustice: Orientations", (2006) 10:3 Lex Electronica at 9, online: <http://www.lex-electronica.org/articles/v10-3/gelinas.htm>.

43 Eisenstein, *supra* note 5 at 51.

44 *Code of Civil Procedure*, R.S.Q., c. C-25, s. 2.

cyberjustice. Such a study has to take into account the cultural, economic, sociological, psychological, political and historical aspects of justice. For example, to what extent is access to justice truly improved by cyberjustice when the "digital divide" is taken into account? Moreover, while the courts are today "one of the most ritualized aspects of social life",[45] the formalities and many rituals of justice will certainly be affected, modified or even eliminated by changes flowing from cyberjustice. Cyberjustice should not be exempt from the rituals that will ensure continuity with more traditional justice.[46] They need to be identified, their functions have to be understood, their underlying reasons have to be analyzed, and the relevance of reproducing or adapting them in a dematerialized environment has to be assessed. At first sight, law does not appear to be the discipline best qualified to grasp these phenomena in a general manner. While the related risks will have a real impact on the law, legal theory may not necessarily be able to explain or establish a comprehensive framework for them. An integrated approach will permit a more harmonious implementation of cyberjustice systems and a more accurate analysis of the impact on society as a whole, from the moment such systems are designed and implemented. The study and consideration of extra-legal consequences inevitably require multidisciplinary research.

CONCLUSION

This article is based on the following premise: implementation of electronic media in the legal field will cause major changes. Yet, even today, over 500 years after Gutenberg, all the consequences of printing have yet to be discovered, in particular with respect to cognition.[47] The study and understanding of the legal implications of cyberjustice systems, which should lead to a definition of their legal framework, are just taking their first steps. The lack of a comprehensive theory for assessing legal risks has caused a disorganization and fragmentation of scholarly work on this issue.

In order to propose avenues for developing such a theory, we have suggested a working definition of cyberjustice that should function across the diversity of cyberjustice systems. The notion of risk must also be studied. Since risk is seen as resulting from human activity and can be traced to the features of artefacts, we have looked in that direction to develop an assessment method. By matching the technological features of cyberjustice systems with the basic values of our justice systems, it is possible to perform a methodical, systematic analysis of the legal risks and

---

45 Claude Gauvard & Robert Jacob, "Le rite, la justice et l'historien" in Claude Gauvard & Robert Jacob, eds., *Les rites de la justice: gestes et rituels judiciaires au Moyen Âge* (Paris: Léopard d'or, 1999) at 9 [translated by author].

46 On this question, see Shulamit Almog, "Creating Representations of Justice in the Third Millennium: Legal Poetics in Digital Times" (2006) 32 Rutgers Computer & Technology Law Journal 183.

47 Eisenstein, *supra* note 5 at 8.

thereby have the capacity to manage them. This does not mean only reducing risk, but also possibly finding a new balance among basic values. Such a study, obviously complex, will help in understanding and grasping the changes envisioned despite their scope.