

**Transactions Related To Internet
Resolving Conflict Of Laws With Reflections In
Unification And Harmonization Of Laws**

Dr. Salah Eldin Gamal Eldin

Ass. Professor And Head of private Law Department

Faculty Of Law And Jurisprudence

Member Of LCIA, AJIA

Abstract:

The information transfer technology represented in the “internet” has had a significant impact on the international trade movement in the past years, and one of the problems raised by these transactions is the problem of conflict of laws or determining the applicable law, which prompted us to prepare this study since the year 2000, which was published in 2004, then Re-write it and publish it in this research in 2020 in proportion to updating the references and opinions that were presented in it, especially since the Internet and the transactions that take place through it have become part of the new world order resulting from the phenomenon of globalization, and then the solution to the problem of conflict of laws was affected by the efforts of unifying and coordinating laws.

We have been exposed to the applicability of national laws, and in it we have been exposed to the applicability of the laws of the United States of America as a law governing online transactions; Due to the existence of the controlling devices on the Internet in this country, and because it is the place of the origin of the Internet, as well as the possibility of applying the rules related to the customs of dealing through the Internet as a subjective law governing these transactions.

This required research on the principle of legality to determine the reasons for finding an organization for online transactions and solving the problem of conflict of laws, and given the diversity of relationships, the study required a study of conflict of laws in the relationship between the Internet user and the service provider, and in the relationship between Internet users themselves before we serve the study by exposure to efforts to unify Coordination of laws at the European level and the global level.

Keywords: Internet, Conflict of Laws, Substantive Laws, Unification of Laws.

المعاملات عبر الإنترنت

مشكلة تنازع القوانين مع إلقاء الضوء على جهود توحيد القوانين

د. صلاح الدين جمال الدين محمد

قسم القانون الخاص، كلية الشريعة والقانون بطنطا، جامعة الأزهر، مصر

ملخص البحث:

صار لتكنولوجيا نقل المعلومات المتمثلة في "الإنترنت" تأثيراً بالغاً على حركة التجارة الدولية في السنوات الماضية، وإحدى المشكلات التي تثيرها هذه المعاملات هي مشكلة تنازع القوانين أو تحديد القانون الواجب التطبيق، وهو ما دفعنا لإعداد هذه الدراسة منذ عام ٢٠٠٠ والتي نشرت عام ٢٠٠٤، ثم إعادة كتابتها ونشرها في هذه البحث عام ٢٠٢٠ بما يتناسب وتحديث المراجع والآراء التي عرضت في ثناياها، لاسيما وأن الإنترنت والمعاملات التي تتم من خلاله صارت جزء من النظام العالمي الجديد الناجم عن ظاهرة العولمة، ومن ثم تأثر حل مشكلة تنازع القوانين بجهود توحيد وتنسيق القوانين.

وقد تعرضنا لإمكانية تطبيق القوانين الوطنية، وفيها تعرضنا لإمكانية تطبيق قوانين الولايات المتحدة الأمريكية كقانون يحكم المعاملات عبر الإنترنت؛ نظراً لوجود أجهزة التحكم في الشبكة العنكبوتية في هذه الدولة، ولكونها مكان نشأة الإنترنت، وكذلك لإمكانية تطبيق القواعد الخاصة بأعراف التعامل عبر الإنترنت باعتباره قانوناً ذاتياً يحكم هذه المعاملات.

وقد اقتضى ذلك البحث في مبدأ المشروعية لتحديد الأسباب الداعية لإيجاد تنظيم للمعاملات عبر الإنترنت وحل مشكلة تنازع القوانين، ونظراً لتنوع العلاقات فقد اقتضت الدراسة بحث تنازع القوانين في العلاقة بين مستخدم الإنترنت ومقدم الخدمة، وفي العلاقة بين مستخدم الإنترنت أنفسهم قبل أن نخدم الدراسة بالتعرض لجهود توحيد وتنسيق القوانين على المستوى الأوروبي والمستوى العالمي.

الكلمات المفتاحية: الإنترنت، تنازع القوانين، القوانين الموضوعية، توحيد القوانين.

Introduction

There can be no single factor, which has such a profound effect on business practices in the last 40 years than the impact of information technology. Which is personified by the Internet, this kind of net which offers us all an exciting chance to exploit new concepts and market opportunities and to push forward the boundaries of existing business relationship⁽¹⁾.

- (1) John Davison: Business and the law on the Internet. A practical guide for J. business managers, Olivier Hans ed. The best at Mc GrowHill, 1996, P. 12. Trazaskowski, Legal aspects of the internet, Al-Borg Univ., 1997, p. 10 - 11 .

The origin of the Internet can be traced back to a project at the U.S. Defense ministry in 1965. The task of the project group "(ARPA)" (Advanced research project Agency) was the development of communication net-work with functioning capabilities which would only be minimally effected in case of a nuclear attack.

CF. Dr. Fritjof Börner and others: The German Internet law Adviser. Legal and Tax implications for E-commerce, Bundesanzeiger, Cologne, 1999, P.17.

Technical description:

The Internet is based on two communication models called transmission control protocol and Internet protocol (TCP/IP). These protocols are a set of standards for data interchange, if the Internet is to be defined on the basis of these protocol, the Internet is the sum of all computers connected to each other with the TCP/IP communication model.

The purpose of the Internet:

Is data transmission or data interchange, data is to be understood as everything that can be digitalized, e.g. data files, pictures, sounds etc.

World Wide Web:

The latest bigger phenomenon on the Internet is the World Wide Web (WWW), which is a new protocol (Called Hyper Text Transmission protocol- HTTP) added to the TCP/IP. The www is based on homepages that can be viewed through a graphic interface called a web browser. This protocol made it way easier to use the Internet, when the old text display was changed to a more entertaining graphical display. The www is the main reason for the enormous growth rates of the Internet, since it was introduced in 1993.

Although the www is part of Internet it is the most used, the fastest

Internet and the phenomena of Globalization:

As economic and social developments all over the world are getting increasingly interconnected the social sciences are being confronted with new issues especially with the changes brought by the globalization⁽²⁾.

One of the consequences for private international law in what concern the new problems created by globalization that we witness increased activities in the field of unification and harmonization of laws in those areas where transactions are inherently world-wide and have little or no connection with a particular legal system. In particular, some transactions related to the Internet⁽³⁾ call for a progressive unification since their roots in a given national system are purely casual⁽⁴⁾. That the Internet ignores international boundaries. "Place" has little meaning in the networked world. With a few exceptions, users are generally unaware that they cross political borders in the course of Internet use". They go through "an international digital journey where the traveler knows neither his destination, nor all of the countries traveled, albeit digitally en route". Moreover, on the World Wide Web we cannot generally discriminate as to who accesses our online material. Even if you want your web page to be read only by Europeans, you can't keep the Americans out. Suddenly, all distribution is global not local.

There can be no doubt that the appearance and particularly the development of global electronic communications, which is sometimes allegorically described as a "global village" or

growing. So it may be used as "incorrect" expression express the Internet.

(2) See Jürgen Basedow: The Effects of globalization on private international Law. In Legal aspects of globalization, KLUER, 2000, P.V & P.2, Globalization has become a very popular word in the social sciences in recent history. It is generally used to describe the fact that an increasing number of social problems have a global dimension today and can no longer be solved by national solutions.

(3) The Internet can loosely be described as the non-controllable net of nets without any central authority. It is unlimited means of communications that allows all kinds activities in virtual cyberspace.

(4) J. Basedow: Op. Cit.,P. 7 and CF. Herbert Kronke: Electronic commerce und Europäisches verbrauchertrags IPR: Recht der internationale wirtschaft. 1996, P. 985.

"Cyberspace⁽⁵⁾", will substantially alter the conditions, Methods and other characteristics of much of our communications.

If so the Internet may cause problems in private international transactions and we have to ask how might we solve these problems in a way that accommodates with not only the uniqueness of the medium, but also the realities of sovereignty and local regulations⁽⁶⁾?

It is logical to study this issue we have to notice that :

The new world order which is to emerge from globalization will be characterized by groups of regulations:

1. World regulations which is most cases will be contained in international conventions;
2. Regional regulations, such as those of the European Union, which may go beyond the model of the international convention and produce a binding effect on the member states and their respective populations.
3. Traditional national regulations,.
4. These regulations which private international law will have to cope with it⁽⁷⁾ and we will detail it in the next pages.

(5) Refers to the interaction of people and businesses over computer network, electronic bulletin boards, and commercial online services. The largest and most visible manifestation of cyberspace is the Internet see R. Timothy muth, old Doctrines on A New Frontier: Defamation and Jurisdiction in cyberspace, Wisconsin State, Law. Sept. 1995, at 11,11.

(6)Markus Fallenböck: Internet und Internationales privatrecht, zu den Internationalen Dimensionen des Rechts im Electronic Commerce, Wien, 2001, P. XX, 226 S

See also, Philip Adam Davis, Indiana Univ., School of Law, The defamation of choice of Law in Cyberspace, Federal Communication Law Journal. Vol. 54, Issue 2, Article 6, p. 339. Spec. P. 341.

Matthew Burnstein: A global Network in compartmentalize legal Environment: in Internet which court syberspace? Which law applies?, K. Boele- Woelk (ed.) Kluwer, 1998, P. 23.

(7) See: basedow. Op. Cit., P. 6.

Section One

The ability to apply substantive law in Internet

The rapid growth of the group known "Internet" or "Cyberspace" users will be accompanied by a growth of regulation.

The main problem of the Internet, Taken from a legally point of view is, that we have a media without any borders and it has to be fitted into a world full of borders and dissimilarity⁽⁸⁾. That is why the problems arising in relation to transnational Litigation consider the most important legal problem when dealing with the Internet, and when this problem is solved the substantive law can be examined.

There are two directions in doctrine around the possibility to regulate the Internet:

While some of doctrines argue that governments should push the architecture of the Net to facilitate its regulation, or else they will suffer a loss of sovereignty⁽⁹⁾, Others encourage community policing as a long-term solution for the healthy development of the Internet⁽¹⁰⁾.

We can discuss these two directions in the next points :

1. Self-Regulation of The internet⁽¹¹⁾

Some commentators said that "private regulation will play a special role on the Internet for two reasons. First, Internet users can by contract choose a single, certain governing law for the particular transactions or networks in question. This alleviates conflicts- of - law difficulties. Second, the value of many Internet transactions is so

(8) See J. Trazaskowski; op. cit. p. 1.

(9) I. Trotter Hardy, "The proper legal regime for cyberspace, University of Pittsburgh Law Review, Vol. 55, 1994, P. 993, Spec, in his Conclusion, P. 1054.

(10) See P.K. Ohm: On regulating the Internet: Use net, A case study, no. 46 U. California Law Review, 1999, P. 1956.

Michele Colucci: The impact of the Internet and New technology on the workplace. A legal analysis from a comparative point of view,(These of P.H.D Univ. of Illinois) Bulletin of comparative labour relations No.43-2002; Editor Roger Blanpain, Kluwer, the Hague., P. 5-6.

(11) In different between self-regulation and non-regulation. See in general : Monroe E. Price and Stebaan G. Vernulot: the concept of self – regulation and the internet, Univ. of Pennsylvania., scholarly commons,2000 , p.1 – 75, spec. p.6.

low that in most circumstances recourse to real- space courts will not be cost- justified".

So, Private regulators can provide dispute resolution mechanisms that are much cheaper less formal than national courts⁽¹²⁾.

To support this point of view They used to use many arguments like:

1. The principal argument against regulation of Internet or "cyberspace" is based on the consideration that government should not impose regulation for problems that could be solved without legislation. In other words the machinery of government should only be deployed to solve problems that private sector cannot solve on its own.
2. Internet regulation does not start from a clean slate, most legal problems related to "cyberspace" already existed in the real world long before. Thus, most of these legal issues are already subject to regulation or can be, at least theoretically, legally resolved by deduction from existing rules⁽¹³⁾.

Then, which legal regime governs a specific transnational electronic commerce transaction can be figured out by applying traditional conflict of law rules and speaking about any efforts to regulate the Internet aim at improving and/or clarifying the existing legal regime governing Internet related activities.

3. Since the Internet network, by design, is decentralized, it cannot be governed⁽¹⁴⁾.
4. Governments have no moral authority to rule, primarily because the governed people do not consent. Moral authority, instead, is vested in the internet internal and informal rule-making bodies⁽¹⁵⁾. In that regard some of authors affirms that: Internet

(12) Jack L. Goldsmith: Against Cyberanarchy, University of Chicago Law Rev., Vol. 65, 1998, p. 146, See also, M.E. Price and Anther: op. cit., p. 12.

(13) F. C. Mayer, Europe and the Internet: the old world and the New medium, EJIL.11 (2000) P. 151 see also Goldsmith, op. cit., p. 199 and David R. Jonson and David post : Law and Borders The Rise of Law in Cyberspace, Stanford Law Rev., May 1996, Vol 48, p. 1357.

(14) P.K. ohm, Op. Cit., P. 1956

(15) J. Perry (Barlow): A Cyberspace Independence declaration, at <http://www>,

communities laws actually have a higher morel authority than those of countries or most other governments, since their member join voluntarily and are free to go⁽¹⁶⁾.

2. Substantive regulations for the internet:

As long as cyberspace was a playground for a small fraction of highly educated people, paid for by large institutions, the myth of an unregulated, independent space or that the Internet could grow. Part of the happy mythology of the network holds that it is a self-regulating entity, controlled by no government- one of the few instances in history of successful anarchy. This was never completely true since most countries have long-standing laws that regulate speech and commerce, irrespective of the medium⁽¹⁷⁾. But which substantive law can govern the Internet?

A. The U.S. Law as applicable law:

The Internet was born in the U.S.A. and the whole Internet architecture still has the marks of its origins as the "U.S." Department of Advanced research project Agency Arpa net⁽¹⁸⁾, most of the relevant software for e-mailing and world wide web (WWW) browsing originates in The U.S, thus reflecting a general U.S-American predominance in computer technology and operating systems. Then the Internet being an American-centered phenomenon, the question arises whether the regulation of the Internet or, more broadly, "Internet governance" automatically has to be more or less an American thing, too?⁽¹⁹⁾

EFF.Org/pub/publications/ John Perry Barlow/Barlow-0296. declaration..

(16) See. M. Colucci, Op. Cit., P. 7.

(17) CF. Global information Networks, Ministerial conference Bonn 6-8 July 1997, 22<[http://www.2.echo.LU/Bonn/Final. Html](http://www.2.echo.LU/Bonn/Final.Html)>. And stephanwilske: international jurisdiction in cyberspace: which states may regulate the Internet?, Federal communication law Journal. Vol. 50, P. 117 Spec. P. 120-121.

(18) Even that, today the technical protocols are established through procedures that are not that directly linked to the U.S any more. See F.C. Mayer, Recht und Cyberspace. Eine Einführung in einige rechtliche aspects des Internet's. Humboldt Forum Recht 3 (1997) at IV, [http://www. Are. Rev. huberlin.de /HFR/3-1997/](http://www.Are.Rev.huberlin.de/HFR/3-1997/)

(19) See Franz C. Mayer: Europe and the Internet: The old world and the New

Europeans hesitate and stress the differences in values, choices and approaches to regulation between the old world and the U.S in general and in the respective attitudes towards Internet regulation in particular⁽²⁰⁾.

"The desire for trust might well lead large firms to establish effective and dependable private legal regimes. But it is still doubtful whether these private regimes will accord with the mandatory laws of territorial governments" and it cannot come close to an adequate response to many Internet regulation difficulties"⁽²¹⁾.

B. The internet Law as applicable Law ⁽²²⁾

Traditional legal commentators treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws. But trying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying. A more legally significant, and satisfying, border for the "law space" of the Net consists of addresses of the machines between which messages⁽²³⁾ and information are routed that separate the tangible from the virtual world.

Many of the jurisdictional and substantive quandaries raised by

Medium. EJIL. 11. (2000) P. 149-169 Spec. P. 149-150.

(20) A Look at recent Internet regulation in the US seems to confirm this assessment, see Freed L. Morrison.: Sex, Lies and Taxes: New Internet Law in the united states, Vol. 41 German yearbook of international Law, (1998) at P. 84.

(21) J. Goldsmith: op. cit., P. 145.

(22) See M. Laguerre : The digital city , The American metropolis and information technology, 2005.

(23) Messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cause or barriers that might otherwise keep certain geographically remote places and people separate from one another, see David R. Johnson and David Post: Law and Borders the rise of law in cyberspace, Stanford law Rev., Vol. 48, (May 1996(P. 1367- 1402).

border- crossing electronic communications could be resolved by one simple principle: Conceiving of cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between cyberspace and the "real world". Using this new approach, we would no longer ask the unanswerable question 'where' in the geographical world a Net-based transaction occurred.

Instead, the more salient questions become: What procedures are best suited to the often unique characteristics of this new place and the expectations of those who are engaged in various activities there?

What mechanisms exist or need to be developed to determine the content of those rules and the mechanisms by which they can enforced? Answers to these questions will permit the development of rules better suited to the new phenomena in question⁽²⁴⁾.

Some commentators argue that the Internet is a separate "place", and that any regulation of this separate place constitutes impermissible extraterritorial regulation and they consider it a bad argument, that the Internet is not a separate place removed from our world. Like the telegraph and telephone, it is a means of transporter communication in which someone in one jurisdiction communicates with someone in another in ways that can cause real- world harms. For example: A book uploaded on the Internet can violate an author's copyright, merchants can conspire to fix prices by e-mail, a corporation can issue of fraudulent security, The list goes on and on. Just about any real- world Trans jurisdictional harm can occur on the Internet. And from the perspective of the regulating nation, the justification for regulation is no different: something it deems bad is happening within its territory, and it seeks to stop it⁽²⁵⁾.

Although of this contradiction: Treating internet as a separate "space" to which distinct laws apply will be "fair to those who pass over the electronic boundary". "It will be much easier to be certain which of those rules apply to your activities on-line than to determine which territorial- based authority might apply its laws to your conduct. For example, you would know to abide by the "terms of service" established by CompuServe or America on-Line when you

(24) D.R. Johnson: Rise of law in Cyberspace, Op. Cit., P. 1378 - 1379

(25) J. Goldsmith : Unilateral regulation of the Internet: A modest defense, EJIL., Vol. 11, 2000, P. 138-139.

are in their online territory, rather than guess whether Germany, or Italy or Egypt will succeed in asserting their right to regulate your activities and those of the "placeless" online personae with whom you communicate⁽²⁶⁾.

C. Conflict between The internet Law and The local territorial

Law:

What should happen when conflicts arise between the local territorial law (applicable to persons or entities by virtue of their location in a particular area of physical space) and the law applicable to particular activities on the Net?

The doctrine of "comity,"⁽²⁷⁾ as well as principles applied when delegating authority to self-regulatory organizations, provide us with guidance for reconciling such disputes⁽²⁸⁾.

It's mean that when a conflict between the laws of two states arises, "each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction, and should defer to the other state if that state's interest is clearly greater." Comity arose as an attempt to mitigate some of the harsher features of a world in which lawmaking is an attribute of control over physical space but in which persons, things, and actions may move across physical boundaries. It functions as a constraint on the strict application of territorial principles that attempts to reconcile "the principle of absolute territorial sovereignty (with) the fact that intercourse between nations often demand(s) the recognition of one sovereign's lawmaking acts in the forum of another."⁽²⁹⁾ In general, comity reflects the view that those who care more deeply about and better understand the disputed activity should determine the outcome. Accordingly, it may be ideally suited to handle, by extension, the new conflicts between the no territorial nature of cyberspace activities and the legitimate needs of

(26) D.R Johnson : op. cit., p. 1380

(27) The legal principle that political entities will mutually recognize each other's legislative , executive , and judicial acts.

(28) Joel R. Paul, Comity in International Law, Harvard Int. L. J., vol. 32, 1991, p.1.

(29) D.R. Johnson: Op. Cit., P. 1392 no 78.

territorial sovereigns and of those whose interests they protect on the other side of the cyberspace border. This doctrine does not prevent territorial sovereigns from protecting the interests of those individuals located within their spheres of control, but it calls upon them to exercise a significant degree of restraint when doing so.

Cyberspace represents a new permutation of the underlying issue: How much should local authorities defer to a new, self-regulating activity arising independently of local control and reaching beyond the limited physical boundaries of the sovereign? This mixing of both tangible and intangible boundaries leads to a convergence of the intellectual categories of comity in international relations and the local delegation by a sovereign to self-regulatory groups. In applying both the doctrine of "comity" and the idea of "delegation"⁽³⁰⁾ to Cyberspace, a local sovereign is called upon to defer to the self-regulatory judgments of a population partly, but not wholly, composed of its own subjects⁽³¹⁾.

Despite the seeming contradiction of a sovereign deferring to the authority of those who are not its own subjects, such a policy makes sense, especially in light of the underlying purposes of both doctrines. Comity and delegation represent the wise conservation of governmental resources and allocate decisions to those who most fully understand the special needs and characteristics of a particular "sphere" of being. Although The Net represents a sphere that cuts across national boundaries, the fundamental principle remains. If the system operators and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government⁽³²⁾.

(30) The idea of "delegation" is something of a fiction. But legal fictions have a way of becoming persuasive and, therefore, real. See, e.g., Lon L. Fuller, *Legal Fictions* 55 (1967). Self-regulatory bodies evolve independently of the State and derive their authority from the sovereign only insofar as the sovereign, after the fact, claims and exercises a monopoly over the use of force.

(31) See Johnson: *Op. Cit.*, P. 1392 (no. 83).

(32) *Ibid.* P. 1393.

The hope for self-government today lies not in relocating sovereignty but in dispersing it⁽³³⁾.

Furthermore, the ease with which individuals can move between different rule sets in Cyberspace has deriving a justification of the State's exercise of coercive power over its citizens from their consent to the exercise of that power. In the nonvirtual world, this consent has a strong fictional element: "State reliance on consent inferred from someone merely remaining in the state is particularly unrealistic. An individual's unwillingness to incur the extraordinary costs of leaving his or her birthplace should not be treated as a consensual undertaking to obey state authority. To be sure, citizens of Egypt, dissatisfied with Egyptian law and preferring, say, rules, can try to persuade their compatriots and local decision-makers of the superiority of the rule-set. However, their "exit" option, is limited by the need to physically relocate to Deutschland to take advantage of that rule set⁽³⁴⁾. In Internet, though, any given user has a more accessible exit option, in terms of moving from one virtual environment's rule set to another's thus providing a more legitimate "selection mechanism" by which different rule sets will evolve over time.

The ability of inhabitants of internet to cross borders as will

(33) The most promising alternative to the sovereign state is not a cosmopolitan community based on the solidarity of humankind but a multiplicity of communities and political bodies- some more extensive than nations and some less- among which sovereignty is diffused. Only a policies that disperses sovereignty both upward (to transnational institutions) and downward can combine the power required to rival global market forces with the differentiation required of a public life that hopes to inspire the allegiance of its citizens .

See , Andrei Savin; Jan Trazakowski, Research handbooks in European Law, Cheltenham, UK; Edward Elgar, 2014, specially part V. Niels Vandezande (Citizens and Internet), p.459.

(34) In Cyberspace, there is an infinite amount of space, and movement between online communities is entirely frictionless. Here, there really is the opportunity to obtain consent to a social contract. Virtual communities can be established with their own particular rule-sets; power to maintain a degree of order and to banish wrongdoers can be lodged, or not, in particular individuals or groups; and those who find the rules oppressive or unfair may simply leave and join another community (or start their own).

between legally significant territories, many times in a single day, is unsettling. This power seems to undercut the validity of developing distinct laws for online culture and commerce: How can these rules be "law" if participants can literally turn them on and off with a switch? Frequent online travel might subject relatively mobile human beings to a far larger number of rule sets than they would encounter traveling through the physical world over the same period. Established authorities, contemplating the rise of a new law applicable to online activities, might object that we cannot easily live in a world with too many different sources and types of law, particularly those made by private (non-governmental) parties, without breeding confusion and allowing anti-social actors to escape effective regulation.

But the speed with which we can cross legally meaningful borders or adopt and then shed legally significant roles should not reduce our willingness to recognize multiple rule sets. Rapid travel between spheres of being does not detract from the distinctiveness of the boundaries, as long as participants realize the rules are changing. It also does not detract from the appropriateness of rules applying within any given place, any more than changing commercial or organizational roles in the physical world detracts from a person's ability to obey and distinguish rules as a member of many different institutional affiliations⁽³⁵⁾, nor does rapid travel lower the enforceability of any given rule set within its appropriate boundaries, as long as groups can control unauthorized boundary crossing of groups or messages. Alternating between different legal identities many times during a day may confuse those for whom Cyberspace remains an alien territory, but for those for whom Cyberspace is a more natural habitat in which they spend increasing amounts of time it may become second nature. Legal systems must learn to accommodate a more mobile kind of legal person⁽³⁶⁾.

(35) See D.R. Jahson: Op. Cit., P. 1400.

(36) See Michael J. Sandel, America's search for a new public philosophy, Atlantic Monthly, Illustrations by Mirko Ilić, Mar. 1996, p. 57- 75 speci. at 74 Beyond sovereign states and sovereign selves ("Self-government today.... Requires a politics that plays itself out in a multiplicity of settings, from neighborhoods to nations to the world as a whole. Such a politics requires citizens who can abide the ambiguity associated with divided sovereignty, who can think and act as multiply situated selves").

In Conclusion, Global electronic communications have created new spaces in which distinct rule sets will evolve. We can reconcile the new law created in this space with current territorially based legal systems by treating it as a distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self regulatory processes, and entitled to appropriate deference- but also subject to limitations when it oversteps its appropriate sphere.

The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, place, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace reflect its special character, which differs markedly form anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an e-mail address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if Cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereigns jurisdiction over "whole," locatable, physical persons. The law of the net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Moreover, if rights and duties attach to an account itself, rather than to an underlying real world person, traditional concepts such as "equality," "discrimination," or even "right and duties" may not work as we normally understand them⁽³⁷⁾.

For example , the types of "properties" that can become the subject of legal discussion in Internet will differ from real world real

(37) For example, when "AOL" America online users joined the Net in large numbers, other Cyberspace users often ridiculed them based on the ".aol" tag on their email addresses- a form of "domainism" that might be discouraged by new forms of Netiquette. If a doctrine of Cyberspace law accords rights to users, we will need to decide whether those rights adhere only to particular types of online appearances, as distinct from those attaching to particular individuals in the real world.

estate or tangible objects, for example, in the real world the physical covers of a book delineate the boundaries of a "work" for purposes of copyright law;⁽³⁸⁾ those limits may disappear entirely when the same materials are part of a large electronic database. Thus, we may have to change the "fair use" doctrine in copyright law that previously depended on calculating what portion of the physical work was copied⁽³⁹⁾. Similarly, a web page's "location" in internet may take on a value unrelated to the physical place where the disk holding that Web page resides, and efforts to regulate web pages by attempting to control physical objects may only cause the relevant bits to move from one place to another. On the other hand, the boundaries set by "URLs" (Uniform Resource Locators, the location of a document on the World Wide Web) may need special protection against confiscation or confusingly similar addresses. And, because these online "places" may contain offensive material, we may need rules requiring (or allowing) groups to post certain signs or markings at these places' outer borders⁽⁴⁰⁾.

The boundaries that separate persons and things behave differently in the virtual world but are nonetheless legally significant. Messages posted under one-e-mail name will not affect the reputation of another-e-mail address, even if the same physical person authors both messages. Materials separated by a password will be accessible to different sets of users, even if those materials physically exist on the very same hard drive. A user's claim to a right to a particular online identity or to redress when that identity's reputation suffers harm, may be valid even if that identity does not correspond exactly

(38) Noting that "original copyright paradigms were created to protect only (physical) books".

(39) Electronic information can be dispensed in any sized serving, ranging from a few words to an entire database. If we use the database as a whole as our measure, then any user's selection will be an insignificant portion. In contrast, if we tried to use the traditional boundaries of the book's cover, the user cannot observe this standard. In some cases it is an entirely theoretical boundary, with respect to material only dispensed from the database. This case demonstrates again that the absence of physical borders between "works" in Cyberspace undermines they utility of doctrines, like copyright law, that are based in the existence of such physical boundaries.

See : D. R. Jonson and others, op. cit., p. 1400, and his notes, no.105- 106.

(40) Ibid. p. 1401.

to that of any single person in the real word⁽⁴¹⁾.

Clear boundaries make law possible, encouraging rapid differentiation between rule sets and defining the subjects of legal discussion. New abilities to travel or exchange information rapidly across old borders may change the legal frame of reference and require fundamental changes in legal institutions. Fundamental activities of lawmaking- accommodating conflicting claims, defining property rights, establishing rules to guide conduct, enforcing those rules, and resolving disputes - remain very much alive within the newly defined, in-challenges the core idea of a current law-making authority- the territorial nation state, with substantial but legally restrained powers.

If the rules of Cyberspace thus emerge from consensually based rule sets, and the subject of such laws remain free to move among many differing online spaces, then considering the actions of Cyberspace's system administrators as the exercise of a power akin to "sovereignty" may be inappropriate. Under a legal framework where the top level imposes physical order on those below it and depends for its continued effectiveness on the inability of its citizens to fight back or leave the territory, the legal and political doctrines we have evolved over the centuries are essential to constrain such power. In that situation, where exit is impossible, costly, or painful, then a right to a voice for the people is essential. But when the "persons" in question are not whole people, when their "property" is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the "citizen" and the "state" changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically defined territories⁽⁴²⁾.

(41) Whether the law should consider that interest to be a "property" right or a right on behalf of the "persona" in question remains in doubt.

- Ibid. p. 1402. J. Trazaskowski, op. cit . p. 20.

(42) Ibid. p. 1402.

Section Two

Legitimacy and Legal reasons to regulate the Internet

It is well accepted today that International law permits a nation to regulate the harmful local effects of foreign conduct. The effects rationale is what justifies nations in unilaterally regulating the harmful local effects of Internet transaction⁽⁴³⁾.

Although of this there are worries that because Internet transactions can appear simultaneously in every jurisdiction, and because nations can regulate the harmful local effects of offshore activity, unilateral regulation of the Internet will lead to multiple and conflicting regulations. This concern is greatly exaggerated for two reasons. One has to do with the limits of enforcement jurisdiction. The other has to do with technological change.

(1) Conflict of regulations in regard to The Limits of Enforcement Jurisdiction:

Although a nation can in theory apply its laws to the local effects of a trans-border transaction, it does not follow that every nation where an Internet information flow appears can regulate that information flow. To understand why, it is necessary to distinguish between a nation's prescriptive jurisdiction and its enforcement jurisdiction. Prescriptive jurisdiction is a nation's power to make its laws applicable to particular transactions. A nation can apply its regulations to an Internet communication that produces harmful local effects. This is prescriptive jurisdiction. But the force of this law- whether or not the regulation is effective- depends on the nation's ability to induce or compel compliance with the law. This is enforcement jurisdiction. The true scope and power of a nation's regulation is measured by its enforcement jurisdiction, not its prescriptive jurisdiction⁽⁴⁴⁾.

For the most part, a nation can exercise enforcement

(43) Jack Goldsmith: op. cit., P. 135- 148 speci.p.138.

He assume that there is no independent substantive international law, such as a human rights treaty. That limits the nation's ability to regulate against local harms as it sees fit.

(44) J. Goldsmith: Op. Cit., P. 139.

jurisdiction only against persons or entities with a presence or assets within its territory⁽⁴⁵⁾. The vast majority of content providers on the Internet have no presence or assets in the jurisdictions that wish to regulate their information flows. They thus need worry only about the regulations of the nation in which they are physically located. Their activities are not subject to multiple regulation, at least not directly so. As a practical matter, the entities potentially subject to multiple Internet regulations are users, systems operators (especially Internet access providers) and transaction facilitators (such as banks and credit card companies) with a presence in more than one regulating jurisdiction. The potential multiple regulatory exposure of these entities is non-insignificant; but the scope of this exposure is far narrower than is commonly thought, and it mirrors the multiple regulatory exposure faced by persons and firms in 'real space'.

But these offshore users with no local assets are generally beyond the regulating nation's enforcement jurisdiction. The Internet users that need to worry about the liability consequences of multiple, conflicting regulatory requirements are persons and firms with a multi-jurisdictional presence⁽⁴⁶⁾.

(2) Conflict of regulations in regard with technological change:

The assumption that a content provider or Internet service provider with a multi-jurisdictional presence cannot monitor or control the geographical flow of information on the Internet. This assumption is false. The architecture of the Internet permits geographical content discrimination. The relevant question is the cost of geographical content discrimination and the desired degree of effectiveness.

To understand the point, It is not true that the web page can be

(45) There are of course exceptions to this general proposition. A default judgment can sometimes be enforced abroad, and extradition is a possibility. I explain why these enforcement strategies are not likely to be relevant to Internet transaction.

(46) Goldsmith: Op. Cit., P. 140.

accessed anywhere in the world, and that there is nothing the web page operator can do to control the geographical flow of his/her information on the Internet⁽⁴⁷⁾. The web page operator can take any steps to ensure that content does not reach an unwanted geographical destination. At the most basic level, she or he can warn users from certain places that access to page's content (be it pornography, a newspaper, a commercial advertisement, a roulette wheel, or whatever) is illegal⁽⁴⁸⁾. Or a multi-state Internet operator can segment web pages geographically and linguistically⁽⁴⁹⁾. Or it can condition access to information on a user's presentation of geographical identification. Many Internet services, for example, require a credit card information to confirm geographical identification. And we see tracking software that confirms the user's geographical identification, as well as digital geographical identification intermediaries akin to age identification intermediaries that already flourish on the Internet. In short, it is quite possible to 'zone' an Internet transmission flow along geographical dimensions⁽⁵⁰⁾. The only question is the cost of geographical discrimination, and the cost is rapidly falling⁽⁵¹⁾.

(47) at a real-space newspaper company that publishes in many jurisdictions.

The newspaper publisher is liable for harms caused wherever the newspaper is published or distributed. A newspaper from state X that publishes in state Y is not allowed to proclaim ignorance of Y's law as a defense when something in the newspaper violates Y's laws governing, for example, copyright or libel. This seems appropriate because, among other reasons, the publisher can control the geographical locus of publication and distribution. The requirement to keep offending content out of a jurisdiction imposes costs on the publisher, who must, for example, keep abreast of regulatory developments in different jurisdictions and take steps to exclude publication and distribution of offending content in places where liability should be avoided. It is thought to be fair and legitimate for a nation to impose this relatively small cost on offshore content providers in order to exclude unwanted content from the territory.

(48) This is a common strategy among gambling and pornographic web pages. Goldsmith: Op. Cit., P. 140.

(49) Both IBM and Amazon. Com employ this strategy, in different ways.

(50) Cf. Lawrence Lessig, 'Reading the Constitution in Cyberspace', 45 Emory Law Review, January, 1995) 869- 910 spec., at 895-899.

(51) It is falling precisely because the threat of multiple regulatory exposure

As the cost of such control continues to drop, and the accuracy and ease of this control increases, Internet content providers in the last years occupied the same position as the 'real-space' newspaper publisher. It became appropriate on the Internet, as in 'real-space', for national law to impose small costs on both types of publisher to ensure that content does not appear in jurisdictions and networks where it is illegal.

If this conclusion seems too strict, it is because we are operating on the assumption that an Internet content provider simply places their content on a web page or e-mail list, not knowing where the content may go and thus not responsible for the harm caused by the content when it enters a jurisdiction that forbids it. It seems that the content provider could not have reasonably foreseen that the content was entering a particular jurisdiction, and thus should not be held liable there. But 'reasonable foresee ability' is a dynamic concept. A manufacturer that pollutes in one state is not immune from the antipollution laws of other states where the pollution causes harm, just because it cannot predict which way the wind blows. Similarly, an Internet content provider cannot necessarily claim ignorance about the geographical flow of information as a defense to the application of the law of the place where the information appears. The nature of the Internet makes it foreseeable that the content might appear anywhere. Whether it is fair to hold a content provider liable in a regulating jurisdiction depends on a complex mixture of what the content provider reasonably should have known about the geographical consequences of its acts, the significance of the extra-jurisdictional harms caused by the acts, and the costs of precautions.

This is why became one of the most important issues concerning transnational liability for Internet transactions become the specification of what reasonable steps an offshore content provider must take to keep offending content out of a regulating

makes it cost-effective for Internet firms to innovate in favour of geographical discrimination).

jurisdiction⁽⁵²⁾. The fairness of the requirement to take steps to ascertain geographical identity will depend, as suggested above, on the costs of doing so-costs that are falling every day⁽⁵³⁾.

It should not have been surprising that with its expansion the Net became relevant to the real world. Legal reality intruded upon the world of Internet: where terms like "rap in Cyberspace"⁽⁵⁴⁾, "Cybertort"⁽⁵⁵⁾, "Cybercrime"⁽⁵⁶⁾ are created, the cry for regulation is not far away. Regulation Finally came to the surprise of "Netizens", not just from the national level.

If we know that Cyberspace doesn't not belong to a single country, but to whole range of countries with diverse legal concepts, and there are many reasons give the governments a motivation to control the Internet, like political aspects, financial aspects (such as taxation), intellectual property rights, trade, it will be normal that many states have an interest in regulating the Internet.

So we can find new regulation in many states, for example: Germany Act on the utilization of teleservices (teleservices Act - teledienstestegetz TDG) of July 22, 1997, amended last by Article I of the bill on legal Frammork conditions for electronic commerce⁽⁵⁷⁾.

This Internet legislation comprises Federal legislation on the "new" Media- the Federal statute on information and

(52) See Goldsmith: Op. Cit., P. 142.

(53) Note that for Internet commercial transactions that involve delivery of real space, as opposed to digital, goods, the Internet firms knows where in real space the product is going and can take steps to keep it from the regulating jurisdiction; the situation is more complicated for the delivery of digital goods),

- See Goldsmith, ibid.

(54) Julian Dibbell, A Rape in Cyberspace (as tinysociety, and How to make one), the village voice, Dec. 21, 1993, at P. 36.

(55) Rosalind Resnick, Cybertort: The New Era, National Law Journal, July 18, 1994, at A1.

(56) Benjamin Wittes, Information- Highway Robbery: is law Enforcement Ready for Cybercrime? Legal Times, Oct. 10, 1994, at P. 16.

(57) Enforced in January 2002.

communication services (IuKdG)⁽⁵⁸⁾ with a teleservices statute (TDG)⁽⁵⁹⁾ on the one hand, and the media services - Interstate - Agreement (MDS+ V)⁽⁶⁰⁾ concluded between the states (Länder) on the other hand. The Federal Electronic signature Act (Signturgesetz) was also part of the IUKDG and was the first digital signature law worldwide to be enacted that covered the whole territory of a state⁽⁶¹⁾.

France should have been well prepared for the Internet, having known since the beginning of the 1980s, a mass- computer phenomenon in some ways similar to the Internet: the Minitel system, which already presented the problems of content control, copyright, identity/ domain name control and all the rest⁽⁶²⁾.

In another scale we can see the European parliament efforts which approved a new copyright rules for the internet . (directive 2019/790 of the EU parliament and of the council of 17 April 2019 on copyright and related rights in Digital Single Market)⁽⁶³⁾.

Also in Australia there is the Victorian legislation "Australia Electronic Transaction act 2000" (VIC) s 7⁽⁶⁴⁾.

Meanwhile, it is hard to maintain that the Net is some kind of free city in the sky by another words "The Internet does not exist in a legal vacuum".

(58) Informations Und Kommunikationsdienstegesetz of 22 July 1997, for an English version see [http:// www. i-id/. de/ rahmen / ivkdge. html](http://www.i-id.de/rahmen/ivkdge.html).

(59) Teledienstegesetz. This statute is laid down in article I of the IUKDG.

(60) Mediendienste - staatsvertrag of 20 January/ 7 February 1997.

(61) Both sets of rules come into force on 1 August 1997.

(62) For more details, see Feral- Schuhl, Cyberdroit. Le droit a L'épreuve de L'Internet, 1999, P 174 et 261, and F.C. mayer: Europe and the internet: The old world and the new medium, EJIL, 11 (2000), 149-169 Spec. P. 154-155. Nicola Lucchi : Access to network services and protection of constitutional Right : recognizing the essential role of inter net access for the freedom of expression, Cardozo Journal of international and comparative Law, VOL. 19. No. 3/2011, p. 645- 678.

(63) See . EUR- Lex , 130, 17 May 2019.

(64) See Act no. 162 of 1999 amended by act 33 of 2011 M De Zwart, "Electronic commerce: Promises problems, and proposals (1998) 21 (2) The University of New South Wales Law Journal (UNSWLJ)308 at 317.

Section Three Principles For Internet Regulation

How to regulate Internet, when individual countries begin to regulate internet, their decisions will reach for beyond their national borders as a result of "the electronic nature of the message transmission"⁽⁶⁵⁾. The question arises her, How we can identifies criteria, which enable a state (like Egypt) to prescribe rules for Cyberspace, to subject violators of these rules to the process of its courts, and eventually to enforce these rules?⁽⁶⁶⁾ and what are the principle bases to prescribe legislations for Internet ?

It is known that Under international law, a state is subject to limitations on its authority to exercise jurisdiction in cases.

Every State has an obligation to exercise moderation and restraint in invoking jurisdiction over cases that have a foreign element, and they should avoid undue encroachment on the jurisdiction of other States⁽⁶⁷⁾. A state that exercises jurisdiction in an overly self-centered way not only contravenes international law, but it can also "disturb the international order and produce political, legal, and economic reprisals"⁽⁶⁸⁾.

(65) Ibid para. 38 see also Stephan wilske: International Jurisdiction in Cyberspace: which stats may regulate the Internet?, Federal communications law Journal, Vol. 50, 1997. P. 117 Spec. P. 125.

(66) Jurisdiction to prescribe means a Stat's authority to make its substantive laws applicable to particular persons and circumstances.

(67) Arthur T. von Mehren & Donald T. Trautman, Jurisdiction to Adjudicate : A Suggested Analysis, 79 HARV. L. rev. 1121, 1127 (1966); Gary B. Born, Reflections on Judicial Jurisdiction in International Cases, 17, Georgia Journal of international & Comparative Law, vol. 17. no. 1, 1987, p. 1- 44, spci. p. 33.

(68) See Barcelona traction, Light and power CO. (Belg. V. Spain) 1970 I.C.J, 3, 17-53 Feb. 5). Traditionally, three kinds of jurisdiction are distinguished: jurisdiction to prescribe, or legislative jurisdiction; jurisdiction to adjudication, or judicial jurisdiction; and jurisdiction to enforce, or executive jurisdiction. Jurisdiction to prescribe is the first step in many analyses. Jurisdiction to adjudicate does not apply in the absence of jurisdiction to prescribe unless the Forum State is willing to apply the law of a foreign State. For jurisdiction to enforce, States also regularly need jurisdiction to prescribe. These distinctions can be important in determining the limits of a country's jurisdictions under international law. Depending on the nature of the jurisdiction being exercised, the requisite contacts with a State necessary to support the exercise of jurisdiction differ.(1) The three types of jurisdiction however, are often interdependent and their scope and

A state has jurisdiction to prescribe law with respect to the principles, which are known as the territoriality principle, the nationality principle, the effects principle, and the protective principle⁽⁶⁹⁾. But we have to note that these principles are not exclusive, that a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connection with another state when the exercise of jurisdiction is unreasonable.

1. Territoriality Principle

“The territoriality principle is by far the most common basis for the exercise of jurisdiction to prescribe, and it has been generally free from controversy.” This principle would allow a State to order service providers who operate on its territory to obey its regulations. It would further allow barring access to certain Web sites from machines operating within the State’s territory. States insist, in fact, on their sovereignty to control activities which happen in their territory even if these activities are not limited to the national territory⁽⁷⁰⁾ even if control might be ineffective⁽⁷¹⁾.

In the CompuServe case, German law was held applicable to bar access for German users to certain news groups. The consequence was that “German law is dictating what British or Egyptian citizens can read and view. This effect, however, was incidental. It was caused by the inability of CompuServe to tailor

limitations are shaped by similar considerations

Bernard H. Oxman. Jurisdiction of States, in ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 277 (Rudolf Bernhardt ed. Installment 10 1987).

(69) See Turkey Internet and E-Commerce investment and business Guide, Strategic information and regulations, 2014. P. 85..

(70) See, e.g. Nathaniel C. Nash, Germans Again Bar Internet Access, This Time to Neo-Nazism, N.Y. Times, Jan. 29, 1996, at D6. The Germany-based T-online service of Deutsche Telekom, a privatized former State enterprise, said it voluntarily blocked access to the World Wide Web site of Ernst Zündel, a Toronto-based Neo-Nazi, after German prosecutors warned the company that they were investigating whether it was helping to incite racial hatred..

(71) Under international law, states can even incur international responsibility if they allow their territory to be used for unlawful activities directed against other states.

CF. Corfu Channel (U.K.V. Alb)1949 I.C.J., 4,22 (Apr.,9).

its services to the laws of each country in which it operates. But it was clear that the CompuServe can not expected to conduct business in Germany free from the application of German laws⁽⁷²⁾.

The territoriality principle, however, would not allow extraterritorial application of national law. An Islamic country, for instance, could legally force a local service provider to comply with a regulation banning access of local users to Salman Rushdie's Satanic Verses. But this principle would not cover an order to remove the controversial novel from the Net in general. Therefore, the attempt of a U.S. agency official in August 1996 to apply the Helms-Burton Act to Internet links from Austria to Iran⁽⁷³⁾ was unlawful under international law.

2. Nationality Principle

The right of a State to regulate the conduct of its citizens anywhere in the world is, like territorial jurisdiction, basically noncontro-versial.

The nationality principle is applicable to juristic as well as to natural persons. As the German branch of CompuServe Inc., for example, is chartered as a German company, it is subject to German law.

In addition to the territoriality principle, therefore, service providers will in many cases also be subject to jurisdiction under the nationality principle⁽⁷⁴⁾.

3. Effects Principle

The effects principle can be invoked when an act committed in one State causes injury in the territory of another State. This principle has been a major source of controversy in antitrust cases where it was invoked to support regulation of activities abroad by foreign nationals because of the economic impact of those

(72) See Terence Gallagher, German Cabinet Approves Internet Regulation, (Dec. 19, 1996) (available at Cyber-Rights Library)
http://snyside.sunnyside.com/cpsr/...9.cr_German_Regulation_of_Internet.

(73) Declan McCullagh, Banning Iran, HOTWIRFED (Aug. 28, 1996)
<http://www.eff.org/~declan/global/iran/hw.iran.082896.txt>.

(74) See in The effects of nationality on company conducts and behavior, specially in transnational relation, Salah Eldin Gamal Eldin, Contracts of technology transfer. Dar Elnahada Alarabia. 1995.

activities in the regulating State⁽⁷⁵⁾. As a basis for jurisdiction however, it is increasingly accepted⁽⁷⁶⁾.

This effect can be seen clearly with regard to E-Mail messages, Bulletin boards and world wide web (www).

a- With regard to E-Mail :

E- Mail Like every other medium, it can be used for illegal activities⁽⁷⁷⁾. In principle, e-mail messages are no different from letters and phone calls, as long as the international character of the communication is known to the sender⁽⁷⁸⁾. Whereas it is more or less obvious that the address is not always clear as to the user's residence. An address at a major commercial Internet service could be associated with a user in Egypt or abroad⁽⁷⁹⁾. That fact, In turn, raises serious questions about the reasonableness of jurisdiction if the sender is not aware of the recipient's country.

In this case, there is no link of the illegal act to the territory of the regulating State and no connection between the regulating State and the sender of the message. The illegal act is not characterized here by any international contact. The assertion of jurisdiction to prescribe is therefore limited to situations in which it is known or at least foreseeable that substantial effects will occur in another State.

(75) INTERNATIONAL CHAMBER OF COMMERCE, The extra-territorial application of national laws. Deter Lange & Gary Born eds. 1987. at 4-32; RICHARD WHISH, COMPETITION LAW 370-385 (3d ed. 1993).

(76) Cf Jason Coppel, A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law, LEIDEN J. Int'l. vol. 6, Issue 1 April 1993. P. 73 – 90, Published online by Cambridge University press. 21 July 2009; Margaret Loo, IBM V. Commissioner: The Effect Test in the EEC, 10 Boston College, INT'L & COMP. L.REV. p. 125 (1987).

(77) See David K. McGraw. Sexual Harassment in Cyberspace: The Problem of Unwelcome E-Mail, 21 RUTGERS COMPUTER & TECH. L.J. 491 (1995); Policing Cyberspace, New Jersey Law Journal, Feb 27, 1995, at 22; E-Mail Is Becoming A Conduit of Prejudice on Many Campuses, N.Y. TIMES, Feb. 16, 1997, at 40.

(78) Cf. in U.S.A. Trotter Hardy, The Proper Legal Regime For "Cyberspace", 55 University of Pittsburgh Law Review, 1994, p. 993- 1053.

(79) See Mark Eckenwiler, Criminal Law and the Internet. Legal Times, Jan. 23. 1995, at 537.

b- With regard to Bulletin Boards:

Messages posted to public bulletin boards pose similar questions of jurisdiction. A writer posting messages containing racism, or hatred in any form knows or ought to know one thing: copies of the message will ultimately be distributed to Internet sites all over the world and messages like this may raise the problem of effects when it contains materials contravening public policy.

c- With regard to World Wide Web:

The Web, a vast decentralized collection of documents containing text, visual images, and even audio clips, poses the greatest problems for international jurisdiction. The Web is designed to be inherently accessible from every Internet site in the world. Information on a Web page resides passively on a particular computer until fetched by a human reader. Even when a Web site's computer can determine the geographical location of the prospective reader's Internet site, that does not disclose the location of the human reader⁽⁸⁰⁾.

Even if the distributor of Sport Illustrated Online Swimsuit Edition is aware that his files are especially attractive for Internet users in Islamic countries where they might be considered indecent, it seems unreasonable to subject this distributor to the decency laws of these countries. The link of the offer to the territory of the regulating State is not obvious. The connection between the regulating State and the distributor is not very convincing. First of all, the distributor will in most cases not even be interested in having his offer spread to exotic countries without a real demand for his products. Additionally, the international community would not recognize a State's pure political or ideological interest in regulating the Internet on a global level. This might be different where the distributor is targeting a certain country with extra efforts.

It seems to be reasonable and justifiable that a country that is targeted in the described way regulates this conduct, thereby subjecting individuals to its laws⁽⁸¹⁾.

(80) Ibid

(81) Cf. INTERNATIONAL CHAMBER OF COMMERCE the extraterritorial Application of national Laws, op. cit., p. 45: extraterritorial regulatory measures generally should be permissible only where both foreign conduct and its effects are constituent elements of the activity to which the national law applies; where the effects within the territory are substantial; and where the effects are a direct and primarily intended result of the foreign conduct.

Section Four

Conflict of Laws and Internet Transactions

The internet is global, So regulations and court decisions that effect it may have extra- territorial effects, in another words, in any dispute over internet activities, a jurisdictional issue (conflict of laws') will inevitably arise because it is hard to identify exactly where transactions, such a e-auctions⁽⁸²⁾ e-contracts... etc, take place⁽⁸³⁾, that the internet is a network of networks consisting mostly of privately – operated network some of thus networks cross national boundaries and many of the organizations themselves cross boundaries too, The invention by a science fiction writer of the virtual world of "Cyberspace"⁽⁸⁴⁾ Merely aids in our conceptual, rather than legal understanding. It dose not help with pinpointing where the exchange of contractual promises takes place⁽⁸⁵⁾. The Internet "pays" no need to geographical or political boundaries. Furthermore, the physical world location of those parts of the Internet infrastructure Via which a communication is carried may be purely Fortuitous"⁽⁸⁶⁾ in most traditional business

(82) Adam Reynolds: E- auction: who will protect the consumer?, Journal of contract Law, Vol,. 18 No I and 2, June 2002, P. 75-106 Spec. P. 89.

(83) That the Internet is a network of networks consisting mostly of privately – operated networks, some of thus networks cross national borders, and many of the organizations themselves cross boundaries too, this fact has important consequences for the choice of law issues to be considered.

Matthew R. Burnstein, conflict on The Net, choice of Law in transnational cyberspace, vanderbelt J. of trans L., vol. 29, Jan., 1996, no1, p.80.

(84) See Pedro De Miguel A Sensio, Conflict of Laws and internet, Elgar information Law and practice(ed.) 2020, Uta Kohl. Conflict of Laws and the internet. The Oxford Handbook of Law, regulation and Technology, Roges Brownword, and Others (ed.) , 2017.

See W. Gibson: Neuromancer, Grafton, London. 1984.

(85) H. Kronke: Applicable Law in Torts and contracts in Cyberspace, in k. Bolele- woelki and G. Kessedjian "eds", Internet. which court decides? Which law applies? Kluwer law international, Boston, 1998, P. 77.

(86) C. Reed; Internet Law; Text and materials, Butierworth, London, 2000, P. 187.

circumstances, it is relatively easy for courts to discern whether or not business is conducted in a particular jurisdiction by simply examining the behavior of the parties. But with internet-conducted affairs, things are more complicated.

The European Commission's Directive on E-commerce⁽⁸⁷⁾ that was derived from the UNCITRAL Model Law on Electronic Commerce indicates that: 'the place of establishment of a company providing services via an internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity.

Unfortunately, the international choice of law is not as developed as the choice of forum, the main regulation in the European Union is the Rome convention, but this convention does only apply to contractual matters⁽⁸⁸⁾.

Each country applies its own principles to determine how it asserts jurisdiction over Internet activities, what law will be applied and whether judgments from other jurisdictions can be enforced. There is no global uniform approach, although similarities do exist between jurisdictions.

In the present nation state system, however, the Legal Framework is built on the basis of sovereignty, territoriality and nationality, private international law is based upon such territoriality of law. According to the choice-of-law rules, any Legal problem is thought to have its (place) in one of the jurisdictions in the real world. Consequently⁽⁸⁹⁾, the Internet

(87) Directive 2000/31/EC of the European parliament and of the council, 2000.

(88) See : A. Sorenson: E-commerce and jurisdiction (2001) : <http://www.misweb.com/Australia-July-Legal>.

(89) See Adam Sataraino; Britain proposed new government powers to regulate the internet to combat the spread of violent and extremist content, Fals information and harmful material aimed at children the New York Times. 7 April 2019.

See also : Hiromi Hayashi and Akira Marums, Japan : Telecoms. Media, & internet 2020, Japanese Act no. 57 of 2003 and its amendment by Act 49 of 2009 and act no. 59 of 2003 , A mended by Act 94 of 2011

provides many interesting problems in the field of private international law⁽⁹⁰⁾.

Especially with the fact that every nation can unilaterally regulate every Internet transaction and the fact that the prospects for harmonization are generally dim in many contexts. This means that the unilateral national regulation will continue to be a primary vehicle of Internet regulation.

Today the problem seems not to be the impossibility of unilateral regulation. The problem seems to be the opposite one of too much unilateral regulation by too many notions⁽⁹¹⁾. It turns out that nations can do lots of things within their territories to affect the cost of, and thereby regulate, transnational Internet communications. And since Internet communications can appear simultaneously in many nations, many nations might assert unilateral regulatory control over Internet transactions. The result is thought to be a conflicts-of-law nightmare, with potentially every nation regulating potentially every Internet transaction.

So, the question of choice of law is "particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty"⁽⁹²⁾.

That the forum's law (Lex Fori) will not necessarily govern the

See also : Linda M. Harasim, Global networks: an introduction, in Global Net works, 1993, P. 2 & 6.

(90) Masato Dogauchi, Law applicable to Torts and copyright infringement through the internet., in Legal aspects of globalization (Jürgen Basedow and Toshiyuki Kono ed.) Kluwer 2000, P, 49. Spec. P. 50.

(91) Jack Goldsmith: Unilateral regulation of the Internet: A modest defense, European Journal of Int'L L., Vol. 11 (2000), P. 135.

(92) See organization for Economic Co-operation and development, Explanatory memorandum, in Guidelines on the Protection of privacy and transborder flows of personal data. 13,36 (1980) and Dan. L. Burk: Patents in Cyberspace: Territoriality and infringement on global computer, Tulane Law Rev. Vol. 68, Nov. 1993. No I. P. 5.

suit⁽⁹³⁾ it is that Forum's choice of law rules that direct the court to the applicable law to achieve maximum Fairness to the parties and to achieve effective implementation and coordination of country policies⁽⁹⁴⁾ by using the required nexus⁽⁹⁵⁾.

But it is not easy to determine this law, that there is no case law or literature dealing with choice of law on the Internet, as example: in contractual disputes in Cyberspace, The domicile of the buyer and the provider is not necessarily of any significance. When buying goods or services on the Internet, which is to be delivered via the Internet, neither of the parties will necessarily be aware of where the other party is domiciled. To describe the complexity of this problem is here an example.

" A Egyptian service provider is providing services from a homepage placed on server in Spain and registered under the Com TLD⁽⁹⁶⁾. The language chosen in English and nothing on the homepage is pointing towards either Egypt or Spain. The buyer is domiciled in U.K. but registered under The. Com TLD, he uses his international credit card to pay for the services and the service is to be delivered via the Internet.

It seem like the contract is concluded between two Americans under the (Com. TLD), but all other factors are pointing somewhere else, but without neither of the parties being aware of it.

(93) John D. Faucher. Comment, let the chips fall where they may: Choice of law in computer Bulletin Board Defamation cases, 26 University of California Davis L. Rev. 1993, p. 1045, spc. 1949.

(94) In case of absence of a coherent choice of law regime we can notes three consequences :

1. Forum shopping which leads to the inconsistent application of law and inconsistent result. Especially in the international context.
2. Diminished predictability due to difficulty in ascertaining what law apply. Particularly in situations such as those occurring in internet and
3. Reduced deterrence because uncertainty as to the applicable law leads to inefficient risk- taking.

(95) A connection or a contacts approach by Finding the natural seat of the matter, by weighing up relevant factors.

(96) Commercial Top Level Domain.

The same example can be used to describe the same complexity in relation to tort, Viz. if the French service provider was publishing defamation or a copyrighted work on the homepage, causing a loss in Egypt.

It seems that the factors for establishing the closest connection will not be clear for the other party.

The question that arises, does their any need for a new choice of law regime to resolve those tricky choice of law questions that arise in this brave new world ? and which kind of ?

In the broadest, most unsophisticated sense, the dispute must be "Internet- related" to be governed by this new model. But that does not go for enough. Simply "Touching and concerning" Internet, however, is not a sufficient reason to invoke an entirely new choice of law Methodology⁽⁹⁷⁾ in anther words, not every dispute need to be controlled by the new choice of law regime. But just those disputes with the required nexus to Internet so as to justify invoking the new model⁽⁹⁸⁾.

With respect to private agreements and the possibility of trading partners choosing the applicable law, several answers indicate that the choice remains impossible in some Countries like Egypt⁽⁹⁹⁾ and Arab worlds and American countries. Provisions in Egypt and Latin American Laws require that a nexus be present in order to decide upon the applicable law. The provisions may be more or less strict about the minimum Linkage rules to be respected. As for jurisdiction, most of these countries have not yet addressed this issue as it applies to e-commerce, although certain respondents stated that this is a serious issue that should be dealt with at the international level⁽¹⁰⁰⁾.

(97) M.R. Burnstein: Conflict on the Net, Choice of law in transnational cyberspace, Vanderbilt J. Trans. L., Vol. 29 Jan. 1996. No. I , P. 75 Spec. P.90. See also, Andreas P. Rindl: Choosing Law in Cyberspace, Michigan J. Int, L. Vol. 19,1998 P. 799 Spec. P. 819.

(98) M. R. Burnstein, op. cit., P. 92.

(99) The Egyptian e-commerce Law is still under discussion in the parliament until January 2020.

(100) Responding to the legal obstacles to Electronic commerce in Latin America, NLCIFT/OAS/BSA conference, Washington, DC Sept. 29- Oct. I, 1999 Issues paper, in Arizona J. int. & comp. Law, Vol. 17, No2, 2000 P.15.

I. The relation between a user and access provider:

There are two levels of connectivity, at the first level a user⁽¹⁰¹⁾ is connected to an "access provider",⁽¹⁰²⁾ which essentially serves as an "on-ramp" to determined the suitable nexus to solve the problems of choice of law we have to distinguish between the information superhighway.

To resolve interuser choice of law problems one of authors⁽¹⁰³⁾ suggested that: (All users might be considered "Citizens" of their access provider. Thus, by reaching Cyberspace through an access provider, it is possible to assign a "Cyber-domicile" to each user. AOL Users are Cyber-domicile America Online, and SO Forth, and then the law applicable will be the law of provider).

2. The relation between the users of the Net:

At this level, a user-through the access provider- becomes part of the larger Cyberspace disputes between the users of internet may be raise contractual liability or tort liability.

1- The choice of law in contractual liability :

A-The express choice of law by forum selection clause:

When "Certainty in contractual obligations is of paramount importance to the parties, the practice of choosing of law by' way of forum selection clause in the contract has become the generally accepted means of handling choice of law for contractual disputes and when litigation will arise from contracts formed, performed and broken in Cyberspace .

The parties have the right to specify which nation's substantive law will govern their contractual rights and duties. So long as the

(101) Users include individuals as well as entitles such as corporations.

(102) Such as the Microsoft Network, CompuServe and America Online (AOL).

(103) Matthew R. Burnstein, Op. Cit. P. 97.

choice is reasonable⁽¹⁰⁴⁾.

There are two important aspects of reasonableness as the national laws normal terms applies to contractual choice of law in Cyberspace:

1. The requirement of "Connecting Factors" to the forum selected, and ...
2. The lack of a gross inequality of bargaining power, such that the choice appears to be oppressive to one party.

The first aspect of reasonableness requires: That, if the national rules of conflict of laws require: The place of contract formation, The place of performance, the domicile either party, the location of the corporate headquarters, or state of incorporation of a party as enough nexus or points of connection, it will not be useful in Cyberspace, specially, it is unclear where some of these locations might be. So, just the domicile of either party is the reasonable nexus which can be used for choosing the law which will govern this contractual relation.

The second aspect of reasonableness requires that the contract's choice of law accurately reflect the intention of both contracting parties; in other words, courts view the selection of law in adhesive contracts⁽¹⁰⁵⁾, So a forum selection clause between a large-scale Internet service provider and its customer is enforceable, even if the access contract between them is a standardized form contract or, perhaps just a visual notice on the log-on screen to the system.

(104) See art. 18 of the Egyptian Civil code (1948).

See G.A. Zaphiriou, basis of the conflict of Laws. Fairness and effectiveness, 10 Georg. Mason. U.I. Rev., 1988, P. 301 Spec. P. 315.

Infaye fangfei wang: internet jurisdiction and choice of law, legal practices in the E.U, U.S and China, Cambridge, Fires ed.2010, p.100, 118-124.

(105) A contract of adhesion is a standardized contract offered exclusively on a "take it or leave it" basis without giving the consumer an opportunity to bargain. Black's Law Dictionary 40 (6th ed. 1990).

B- The implicit choice of law for contracts without a forum selection clause :

The choice of law for contract disputes in the absence of a forum selection clauses, poses difficulties. without a forum selection clause, the choice of law for a contractual dispute devolves upon the law of that nation most closely connected with the relevant contractual issue.

But how we can determine this connection in the absence of a valid stipulation of the applicable law by the parties?

Most of legislations refer to the "place" and "Location" of certain events, when "place" or "Location" mean little or nothing in cyberspace contracts.

Even art. 4 of the 1980 convention on the law applicable to contractual obligations (Rome Convention), it is requires that, in the absence of express or implied choice, a contract be "governed by the law of the country with which it is most closely connected".

It is easy to envision a scenario in which a contract between a commercial internet provider and a newsgroup manger is formed in internet, payment is electronically made cyberspace, and performance is accomplished by services rendered in cyberspace⁽¹⁰⁶⁾.

Localization difficulties in the internet :

One of the fundamental difficulties which we face in determining the applicable law is the localization of a transaction which is effected via the internet. Could we apply traditional localization principles to transaction which is effected via the internet ?

Doing so requires an Identification of the physical place where the appropriate element of the transaction occurred, as a consequence of which jurisdiction is awarded to the state in whose territory that place is Located, or its law is applied.

This produces workable answers for most physical world

(106) See for example : the case cubby v. CompuServe, 776 f. supp. 135 (S.D.N.Y.1991, a cyber-defamation case), CompuServe had contracted with Cameron communications, inc. assume editorial control over the content of the information transmitted on the bulletin board . Cameron then subcontracted this work to anther company- DFA . in cyberspace : liability on the electronic frontier, computer law, July, 1994, at 2-3.

transactions. As we shall see, however, the likely result of applying the concept of localization to an electronic commerce or Internet transaction is either :

- the applicable law or jurisdiction is potentially that of every country in the world; or ...
- the applicable law or jurisdiction is purely fortuitous, and has no obvious connection with the parties or the substantive transaction.

This can be demonstrated by applying the localisation principles of the various international conventions on private international law to examples from real-life electronic commerce or Internet transactions.

* Place of supply of goods, services or performance of principal obligation:

There are numerous provisions in the convention of 1980 relating to the applicable law or jurisdiction for contracts which specify the place of supply as a localization trigger. Whether a sensible result is produced depends on the subject-matter of the contract, Thus where the contract is to supply physical goods (ie., the electronic commerce transaction is simply an equivalent channel to mail or telephone ordering) the localization of the contract presents no special problems: the relevant place is the address for delivery of the goods.

However, the position is quite different if the contract is for a 'product' which is to be delivered electronically. The most obvious of such products are on-line services, and information products (eg software, images, music, video or games). For these, the place of supply is hard to define. The options are as follows:

The place of electronic "delivery" of information products and services is an elastic concept, which depends very much on the supply technology used. For example:

- If the product is sent as an email attachment, its place of receipt will probably be determined in the same way in which the courts would decide where a contractual acceptance was received. Taking the example of a purchaser who is employed in London by a multinational corporation whose domain name points initially to a server in the US,' there are at least three possible places of receipt:

- If the place of receipt is the moment the message enters the corporation's systems (as would probably be the case under eg art 1335 of the Italian Civil Code), the relevant location would be the US, ie the physical location of the server to which the corporation's domain name points. We must also note that this server could at any time be moved to a different physical location, in any jurisdiction, without affecting the operation of the email process. and without the sender or recipient realizing the fact.
- If the place of receipt is at the purchaser's mailbox, this would probably be located on a UK-based server to which the email is routed by the corporation's internal network. However, there is no technical reason why the corporation might not, without this being apparent to the purchaser or the vendor, physically relocate that server to eg Guatemala. The system would perform in an apparently identical way so far as both parties are concerned.
- If the place of receipt is where the purchaser actually downloads and/or reads the email, that could occur in whichever jurisdiction he or she happened to be located when the email was collected from the mailbox. The place of downloading and the place of reading could also be different, eg if the purchaser downloads email to a laptop in London but does not read it until arrival in Paris⁽¹⁰⁷⁾.

Time of acceptance is either the entry of the communication into the system denoted by the recipient (eg the email host) or, if none is designated, the time when the communication actually comes to the attention of the recipient. In the context of the Internet the second opinion will rarely apply, as it is usually impossible to communicate with a person without knowing the address of the relevant system⁽¹⁰⁸⁾.

* Place where purchaser took steps towards contract formation:

The place where the purchaser took these steps may be one of

(107) The Australian Electronic Communications Act 1999 does not deal with this issue directly, but offers two possible analogies by making provision in S 14 for the time and place of receipt of an electronic communication.

(108) Chris Reed : internet Law, text and materials, Butterworth London, 2000, p.192- 194.

the jurisdictions in which an action. can be brought, though often only if the purchaser is the habitually resident there. At first sight this presents fewer difficulties, as the physical location of the purchaser can usually be determined with some certainty.

Even here, however, problems can arise :

- The purchaser begin the transaction in one jurisdiction and complete it in another. Some electronic commerce suppliers allow customers to start partial orders and return to them at a later date to complete the order.

- The purchaser is 'visiting' a different location, and the applicable the (an equally difficult question) determines that the contract-forming actions took place on that website, and not at the user's computer.

* State where, supplier's branch, agency etc. is established:

In the field of regulated services, such a banking and financial services, some commentators have suggested that whenever a person accesses the supplier's website, a temporary, virtual, branch is created. If this argument is accepted, it means that each electronic commerce business has, at some time or other, established a branch in every jurisdiction of the world where Internet access is possible.

* " Targeting ":

An approach which at first sight seems attractive is to grant jurisdiction to those jurisdiction whose residents are targeted by the supplier. The justification for this approach is that the supplier is seeking customers in that jurisdiction, and can thus hardly complain if its courts claim jurisdiction over his activities, some authors who call to internet new legal framework for internet said that, attempts to resolve choice of law question in contractual disputes by reference to " close connection " are unhelpful ; According them, We have to return to the new " Lex Mercatoria " to determining the law applicable to contacts disputes arising through contractual relations in internet⁽¹⁰⁹⁾.

(109) See trotter Hardy : The proper legal regime for cyberspace, univ., Pittsburgh L. Rev., 1994, P. 933 and Matthew R. Burnstein ; op. cit. p.75 .

2- Choice of law for tort liability :

Because no multinational agreement exists with regard to torts in the internet, choice of law for torts has focused on two theories:

- (1) The lex loci delicti approach.
- (2) The most significant relationship approach .

(1) The lex loci delicti approach.

Some of nations still follow the simple choice of law rule that is almost mechanical in it's operation, the rule of lex loci delicti, The law of the place of the wrong. The place of the wrong is the state where " the last event necessary to make an actor liable " for an alleged tort takes place⁽¹¹⁰⁾.

In transnational cyberspace, however, the place of the wrong might be any of the 145 – plus nations that are on line⁽¹¹¹⁾. More accurately, there is no lex loci delicti⁽¹¹²⁾. The state of the last act is ordinarily the state where injury occurs.

If injury occurs in cyberspace. it can be said that the place of the wrong is cyberspace itself⁽¹¹³⁾. Because there is no single answer to this choice of law problem, the forum will likely apply its own law to the dispute⁽¹¹⁴⁾. This lex fori default rule, of course, encourages forum shopping.

The traditional rule is an adequate one in real space because

(110) See generally J. D. Lee & Barry A. Lindahl, Modern tort law : Liability & Litigation west group ed. § 13.03, 1988, Rev. ed. 1994.

(111) See John D. Faucher : Comment, Let the chips fall where they may : choice of law in computer Bulletin Board defamation cases, 26, U. C. Davis L. Rev. (1993) p. 1045 sec. p. 1050- 1057 .

(112) See Hamilton De Saussure & p.p.c Haanappel, A Unified Multinational Approach to the application of tort and contract principles to outer space, 6 Syracuse J. Int'l L. & Com. 1. 12 (1978) " For outer space, there is no lex loci delicti commissi. Thus this venerable rule, so generously applied in both common and civil law countries, is impossible to follow for space related torts ".

(113) For example. many users employ pseudonyms on the Internet. Conceptually, if true anonymity exists and the pseudonymous character In cyberspace Is defamed. Is there any injury per se in real space? In this light. cyberspace creates the possibility for injury only in the virtual sense.

(114) Forum shopping enables a plaintiff to achieve more favorable ruslts by choosing to sue in one forum and receiving the benefit of that forum' substantive law. Blak's Law Dictionary 655, 6th ed. 1990 .

of its certainty and ease of application. But the numerous reveal that one cannot easily identify "where" events transpire on the Internet and " it (Lex Loci delicti) is not a sound choice of law regime for cyberspace "⁽¹¹⁵⁾.

In the conclusion "Lex Loci dilicti and the most significant relationship analysis- break down on a globally interconnected information superhighway ".⁽¹¹⁶⁾

(2) The most significant relationship approach .

In this approach to choice of law, legislature give list of the variety of contacts to be considered such as : The place of injury, the place where the conduct causing the injury occurred, the place of domicile or residence of the parties, and the place where the parties, relationship is centered⁽¹¹⁷⁾. But how we can use this geographically oriented principles to determined the applicable law in torts through cyberspace ?

It is apparent that this approach does not afford much guidance to a court attempting to choose the appropriate law; some factors might weight toward one forum, others to another. The question which still without answer : How are the relevant factors to be considered in transnational cyberspace ?

Or : how are contacts such as the place of injury, place of conduct causing injury, and nationality determined in the network world?

Here also, some authors invite to A new choice of law regime for transnational cyberspace which should serve the twin goals of conflict of laws : " certainty and fairness"⁽¹¹⁸⁾.

(115) See Linda O. Simddy : Choosing the law and forum for the litigation of disputes, in "toward a law of global communication networks" 299 (Anne W. Branscomb ed. 1980.

(116) M. R. Burnsteini : conflicts on the net. op. cit., p. 96.

(117) See as ex : Egyptian Civil Law no 48 – 1948, art 19.

(118) George A. Zaphiriou, Basis of conflict of laws : Fairness and Effectiveness. 10 Geo. Mason u.l. Rev. 302 – 303(1998) and M. R. Burnstein . op. cit, p. 75- 116 spci. P. 95.

Section Five

Harmonization of Regulations of Internet

Harmonization of Law aims to create consistency of Laws, regulations, standards and practices, So that the same rules will apply to businesses that operate in more than one state, This which can used in activities which flow through the Internet (e- contract, e- signature, copyright, mobile payment etc.)⁽¹¹⁹⁾.

When regulatory conflict and regulatory spillover occur with respect to 'real-space' transnational transactions, nations have responded with a variety of international harmonization strategies. Sometimes harmonization takes the 'hard' form of treaties that either establish a uniform international standard, or an international anti-discrimination regime, or an international choice-of-law regime. Other times harmonization takes 'softer' forms like information sharing among enforcement agencies or informally agreed-upon regulatory targets⁽¹²⁰⁾.

Various harmonization strategies are being employed to address the challenges of regulating the Internet. Consider a few examples. Several recent treaties and related multinational edicts that have strengthened digital content owners' right to control the distribution and presentation of their property online⁽¹²¹⁾. So, Harmonization strategies could seen in activities of several international organizations which have drafted model laws and guidelines to facilitate Internet commerce and related digital certification issues.

Harmonization strategies such as these are clearly an important response to the jurisdictional difficulties of Internet regulation. If

(119) See UNCTAD : Harmonizing Cyberlaws and regulations, The experience of the East African Community, 2012. 66 pages.

(120) See Michael Chertoff and Paul Roseenzweig : A primer on Globally Harmonizing internet Jurisdiction and regulations, CIGI, Ontario, Canada, Global Commission on unilateral Governance, Proper Series : No. 10, March 2015.

See also : J. Goldsmith , unilateral regulation of the internet, a modest defense, European Journal of international law (E.J. I. L) , 2000, Vol. 11, no. 1, p.135- 148, spec. p. 146.

(121) Like copyright regime and e - commerce.

successful, these strategies can reduce or even eliminate the costs of regulatory conflict. But public harmonization is not a panacea. It is useful to recall, in this regard, that there are good reasons for regulatory difference among nations. Nations have different regulatory commitments because of, among other things, differences in endowment, technological capacities, and preferences. A primary virtue of decentralized lawmaking by nation states (as opposed to uniform international rules) is that it allows populations to implement policies that reflect these differences. This in a nutshell is the theory that informs, among other things, the concept of national sovereignty, the European principle of subsidiary, the American conception of federalism, and the economic concept of comparative advantage. In addition to these 'substantive' differences among nation, there is 'procedural; value in having decisions made at the smallest possible political unit.

These substantive and procedural values are diminished by international harmonization. They are costs to be weighed in the balance when considering the virtues of harmonization, especially since some harmonization efforts reflect coercion by powerful nations rather than truly fair or efficient regulatory improvements. In addition, these considerations suggest why harmonization is often not easy to achieve. When regulatory difference reflects important local values, harmonization is hard because of (among other things) domestic political opposition. This is why so many international regulatory regimes are littered with (usually ill-defined) mandatory or local public policy exception⁽¹²²⁾. This fact should give harmonization's champions pause when addressing national differences in the Internet context concerning privacy, free speech, consumer protection, competition policy and the like.

It is difficult to generalize about when harmonization of Internet-related regulations will be successful, for the Internet covers a broad range of regulatory concerns. We can probably

(122) For example, the New York convention, the Convention on the International Sale of Goods, the Rome Convention, and so on.

expect relatively robust harmonization in those contexts- like consumer fraud- where nations' interests converge and the gains from cooperation are high⁽¹²³⁾. Harmonization is also likely in coordination situations- such as the communication protocols that define the Internet- where every nation has an incentive to adhere to the adopted standard. The particular standards adopted of course have distribution consequences, which usually mean that powerful nations determine their content; but after the standard is adopted, all nations have incentives to adhere to it. This type of coordination situation, it must be admitted, is not likely to be present when contested social values are in issue.

In many other situations, harmonization will either be undesirable or impossible to achieve. In these situations unilateral regulation will remain the primary method of public regulation.

- Harmonization efforts and conflict of laws:

Scholars who study conflict of laws are used to regulatory conflict. They are less likely to see it as the unalloyed evil that other scholars see because they realize that it is often normatively preferable harmonization and that it is in any event often inevitable. With this thought in mind, it is important to see that the threat of multiple regulatory exposure will not, as many once histrionically claimed, destroy the Internet. The threat of multiple regulatory exposure is simply a cost of doing business on the Internet, a cost that has not prevented enormous Internet growth in recent years⁽¹²⁴⁾.

- Harmonization efforts in European Union:

Most of the efforts at the level of the European Union started in the 1990s, when the Internet became a mass phenomenon. The standard approach at the EU level, so far, has been to regulate specific aspects of the Internet related to the mainly economic⁽¹²⁵⁾

(123) J. Goldsmith Unilateral regulation.... Op. Cit., P. 147.

(124) For another , preview, see, Antonio Segura Serrans, international regulation of the internet, Oxford Bibliographics, 25/9/2019, See also, in general : Kittichaisaree, Kriangsack, public international law of cyberspace, Cham, Switzerland, Springer 2017.

(125) See J. Dickie, Internet and Electronic Commerce Law in the European

field of European integration.

The earlier regulatory efforts were not specifically aimed at the Internet but were more general efforts to regulate multimedia activity⁽¹²⁶⁾. Those efforts became more and more Internet specific during the second part of the 1990s⁽¹²⁷⁾. The draft directives on digital signature and on electronic commerce probably contain the

Union Hart publishing, England, (1999) 3 and seq. See also Europe and Internet , the old World and The new medium, E.J.I.L, 11, 2000, P. 149 - 169 Spec. P. 156. and See Directive 95/461 EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (O.J) 1995L 281/31) may be a typical example. The directive states that the free movement of data is closely related to the free movement of goods and services and that data are goods requiring specific protection. The directive is closely linked to the Internet as the Internet is probably today's most important sector for data transfer. The Commission Green Paper on "The Protection of Minors and Human Dignity' (COM (96) 483) published in October 1996 together with a communication concerning illegal content on the Internet is one of the few documents focusing on non-economic issues. Cf. Also the Council resolution of 17 February 1997, OJ 1997 C 70 and the recommendation of the Council on the protection of minors and human dignity, pointing to auto-regulation, of 24 September 1998, 98/560/EC most recently the draft resolution concerning child pornography on the Internet, OJ 1999 C 362/8 et seq.

(126) Klawns W. Grewlich, "Cyberspace": Sector-specific Relation and Competition Rules in European Telecommunication', Common Market Law Review VOL.36,(1999) p. 937-969.

(127) For directives not directly aimed at the Internet but having strong impact on Internet governance see Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997L 144/19) with financial services being subject to special directive (COM (98) 469); cf. Also the draft directive on copyright protection (COM (97) 628); Directive 96/9/EC of 11 March 1996 on the legal protection of databases (OJ 1996L 77/20); Directive 98/84/EC on conditional access systems (OJ 1998L 320/54); Directive 98/34/EC (OJ 1998L 204/37) and Directive 98/48/EC (OJ 1998L 271/18) aim at preventing regulatory fragmentation in the field on information society services through a mechanism the requires Member States to inform the Commission about any national regulation that concerns information society services.

most specific Internet rules issued by the EU and as such they are worth a closer look.

1. Digital Signature:

Facing increased legislative activity in the area of digital signature and encryption, the European regulation No. 910/2014, Known as The electronic identification and trust services for electronic transactions (eIDAS regulation) went into Force on July 2016 having " direct effect – in other words – being Mandatory and wholly adopted in all members states, with precedent over any conflicting national laws⁽¹²⁸⁾.

The Commission detected a need for a harmonized legal framework at the European level in order to avoid the development of obstacles to the functioning of the Internal Market in 1997. The approach chosen⁽¹²⁹⁾ included posterior authorization, voluntary accreditation schemes, a focus on the essential requirements for certifications service providers, including their liability. The Commission emphasized the need to take into account ongoing developments at the international level such as the United Nations Commission of International Trade Law (UNCITRAL) Model Law on Electronic Commerce and subsequent work aimed at the preparation of uniform rules on digital signatures,⁽¹³⁰⁾ OECD work following the 1997 Guidelines for Cryptography Policy and WTO activities.

2. Electronic Commerce:

The issue of electronic commerce⁽¹³¹⁾ led to one of the most important and probably also most ambitious efforts of the European Commission to regulate the Internet. After its electronic

(128) It replaces the e-signature directive 1999/93/EC

(129) OJ 198 C 325/5 et seq.; cf. Also Brisch, 'Gemeinsame Rahmenbedingungen für elektronische Signaturen', CR (1998) 492; Directive 1999/93/EC of 13 December 1999, OJ 2000 L 13/12 et seq.

(130) Draft rules on electronic signatures have been published in November 1998, see <http://www.un.or.at/uncitral/english/session/wg-ec/wp-79.htm>.

(131) For a general overview on electronic commerce, see Stoll and Goller, 'Electronic Commerce and the Internet', 41 GYIL (1998) 128, Lornia Gillies, electronic commerce and international private law : A study of electronic consumer contacts, 2008.

commerce communication 'A European Initiative in Electronic Commerce' of April 1997⁽¹³²⁾, the Commission put forward a proposal for a directive on electronic commerce in November 1998⁽¹³³⁾, aiming at establishing 'a coherent legal framework for the development of electronic commerce within the Single Market'⁽¹³⁴⁾, and This is proposal which become the directive 2000/31/EC of the European parliament and of the Council & June 2000 on certain legal aspects of information society services in particular electronic commerce, in the internal market (Directive on electronic commerce)⁽¹³⁵⁾; to remove obstacles to the cross- border online services in the EU and provide legal certainty to business and citizens.

The country-of-origin principle as an established principle of EC law is the leading principle of the draft directive. Generally speaking, it is applied when harmonization of rules is either not feasible or not desired

The directive defines the place of establishment in line with the principles established for Article 43 (ex 52) ECT⁽¹³⁶⁾ as the place where the operator actually pursues an economic activity through a fixed establishment, irrespective of where websites or servers are situated or where the operator may have a mail box. The aim of those provisions is to remove legal uncertainty and to ensure that operators cannot evade supervision, as they would be subject to supervision in the Member State where they are established. In addition, information service providers are obliged to make available to customers and competent authorities basic information in an easily accessible manner and in a permanent form concerning

(132) COM (97) 157.

(133) COM (98) 586, see OJ 1999 C 30/4.

(134) Press release DG XV, available at

http://www.europa.eu.int/comm/dg_15/en/media/elecomm/999.htm

(135) OJL 178, 17. 7. 2000, p. 1- 16 .

- <http://data.europa.eu/eli/dir/2000/31/OJ>

(136) See Case C-221/89, Factortame (1991) ECR(European Congress Review) 1-3905.

their activities (name, address, e-mail address, trade register number, professional authorization and membership of professional bodies where applicable, VAT number).

The directive requires Member States to adjust national legislation with a view to removing any prohibitions or restrictions on the use of electronic media for concluding contracts.

The directive is silent on whether this implies the respective municipal conflict-of-law rules, which could bring an activity under a different legal regime, than the one of the country of origin⁽¹³⁷⁾.

- Harmonization of legal rules:

Since it is proven pretty difficult to agree on a common legislation on the private international law, another approach has been used, viz. harmonizing the substantive law⁽¹³⁸⁾.

In other words, The problem of conflicting legal rules may be solved by harmonizing, at a minimum, the substantive laws governing the Internet on a worldwide basis or at least at a regional one⁽¹³⁹⁾ especially if we notice that uniform law is never comprehensive. Gap and exceptions from its scope of application cannot be avoided altogether. Courts have traditionally filled these gaps by having recourse to a national law, either the Lex Fori, or more correctly, the Lex causae.

In practice this method of composing the applicable law from two sources, i.e. the convention and the national law, has turned out to be overly complicated and to threaten the uniform enforcement of the convention. More recent conventions have therefore introduced an intermediate level of rules between the convention and national law: The general principle of law⁽¹⁾.

Recourse to the applicable national law can only be had where such principles are absent⁽²⁾.

(137) See Hoeren, *supra* Op. Cit., at 195.

(138) J. Trazaskowski: Legal aspects, Op. Cit., P. 31.

(139) See: European directive of 2014 and its amendment of 2018. See also notes of M.Colucci, *The Impact of the Internet.*, 2002, Kluwer, PP. 9-10.

(1) See Art. 7 of the UN sales convention.

(2) J.Basedow: Op. Cit., P. 7.

Conclusion

I agree with some commentator ⁽¹⁾ that internet transactions are not different from real space transnational transactions.

That internet transactions are not different from real space transnational transactions.

They involve people in real space in one jurisdiction communicating with people in real space in other jurisdiction in a way that often good , but sometimes causes harm. There is no general normative argument that support the immunization of cyberspace activities from territorial regulation. And there is every reason to believe that nations can exercise territorial authority to achieve significant regulatory control over cyberspace transactions. Resolution of the choice of law problems presented by internet transactions will be challenging, but no more challenging than similar problems raised in other transnational contexts.

(1) Jac L. Goldsmith , Against cyber anarchy, University of Chicago Law school, Vol. 65: P. 1199. 1998.

BIBLIOGRAPHY**❖BOOKS :**

- 1- **Antonio Segura Serrans** : international regulation of the internet, Oxford Bibliographics, 2019
- 2- **Bernard H. Oxman**: Jurisdiction of States, in ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 277 (Rudolf Bernhardt ed. Installment 10 1987).
- 3- **Blak's Law Dictionary** 655, 6th ed. 1990 .
- 4- **Chris Reed** : internet Law, text and materials, Butterworth London, 2000, p.192- 194.
- 5- **Fritjof Börner and Others**: The German Internet law Adviser. Legal and Tax implications for E-commerce, Bundesanzeiger, Cologne, 1999.
- 6- **Herbert Kronke**: Electronic commerce und Europäisches verbrauchervertrags IPR: Recht der internationale wirtschaft. 1996.
- 7- **Hiromi Hayashi and Akira Marums**: Japan - Telecoms. Media, & internet 2020.
- 8- **Infaye fangfei wang** : internet jurisdiction and choice of law, legal practices in the E.U, U.S and China, Cambridge, First ed. 2010.
- 9- **J. D. Lee & Barry A. Lindahl**: Modern tort law , Liability & Litigation west grouped. 1988, Rev. ed. 1994.
- 10- **J. Dickie** : Internet and Electronic Commerce Law in the European Union Hart publishing, England, (1999).
- 11- **Jac L. Goldsmith** : Against cyberanarchy, University of Chicago Law school, 1999.
- 12- **Pedro De Miguel A Sensio**: Conflict of Laws and internet, Elgas information Law and practice(ed.) 2020,
- 13- **Salah Eldin Gamal Eldin**: Contracts of technologie transfer. Dar Elnahada Alarabia. 1995.
- 14- **Sorenson**: E-commerce and jurisdiction (2001) :
- 15- **UNCTAD** : Harmonizing Cyberlaws and regulations, The experience of the East African Community, 2012.

❖ Articles :

- 1- **Adam Reynolds:** E- auction: who will protect the consumer?, Journal of contract Law, Vol., 18 No I and 2, June 2002, P. 75-106.
- 2- **Andreas P. Rindl:** Choosing Law in Cyberspace, Michigan J. Int. L. Vol. 19,1998.
- 3- **Benjamin Wittes:** Information- Highway Robbery: is law Enforcement Ready for Cybercrime? Legal Times, Oct. 10, 1994.
- 4- **CF Jason Coppel:** A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law, LEIDEN J. int'll. vol. 6, Issue 1 April 1993
- 5- **Computer law,** July, 1999, at 2-3..
- 6- **David K. McGraw:** Sexual Harassment in Cyberspace: The Problem of Unwelcome E-Mail, 21 RUTGERS COMPUTER & TECH. L.J. 491 (1995); Policing Cyberspace, New Jersey Law Journal, Feb 27, 1995, at 22; E-Mail Is Becoming A Conduit of Prejudice on Many Campuses, N.Y. TIMES, Feb. 16, 1997, at 40.
- 7- **David R. Johnson and David Post:** Law and Borders the rise of law in Cyberspace, Stanford law Rev., Vol. 48, (May 1996).
- 8- **Declan McCullagh:** Banning Iran, HOTWIRFED (Aug. 28, 1996).
- 9- **F.C. mayer:** Europe and the internet: The old world and the new medium, EJIL, 11 (2000), 149-169 Spec.
- 10- **Feral- Schuhl:** Cyberdroit. Le droit a L'épreuve de L'Internet, 1999,
- 11- **Franz C. Mayer:** Europe and the Internet: The old world and the New Medium. EJIL. 11. (2000) P. 149-169.
- 12- **Freed L. Morrison:** Sex, Lies and Taxes: New Internet Law in the united states, 41 German yearbook of international Law, (1999) at 84.
- 13- **G.A. Zaphiriou :** basis of the conflict of Laws. Fairness and effectiveness, 10 Georg. Mason. U.I. Rev., 1988.
- 14- **Goldsmith, Unilateral :** regulation of the internet, a modest defense, European Journal of international law (E.J. I. L) , 2000.
- 15- **Goldsmith J., David R. Jonson and David post :** Law and

- Borders The Rise of Law in Cyberspace, Standford Law Rev., Vol 48, (May 1996).
- 16- **H. Kronke:** Applicable Law in Torts and contracts in Cyberspace, in Bolele- woelki and G. Kessedjian "eds", Internet. which court decides? Which law applies? Kluwer law international, Boston, 1998.
 - 17- **Hamilton Desaussure & p.p.c Haanappel:** A Unified Multinational Approach to the application of tort and contract principles to outer space, 6 Syracuse J. Int'l L. & Com. 1. 12 (1978)
 - 18- **John Davison:** Business and the law on the Internet. A practical guide for business managers, Olivier hans ed. The best at Mc GrowHill, 1996.
 - 19- **jürgen Basedow:** The Effects of globalization on private international Law. In Legal aspects of globalization, KLUER, 2000
 - 20- **Michele Colucci:** The impact of the Internet and New technology on the workplace. A legal analysis from a comparative point of view,(These of P.H.D Univ. of Illinois) Bulletin of comparative labour relations No.43-2002; Editor Roger Blanpain, Kluwer, the Hague.
 - 21- **Trazaskowski,** Legal aspects of the internet, Al-Borg Univ., 1997.
 - 22- **Uta Kohl:** Conflict of Laws and the internet. The Oxford Handbook of Law, regulation and Technology, Roges Brownword, and Others (ed.) , 2017.
 - 23- **W. Gibson:** Neuromancer, Grafton, London. 1984.
 - 24- **John D. Faucher.** Comment, let the chips fall where they may: Choice of law in computer Bulletin Board Defamation cases, 26 University of California Davis L. Rev. 1993.
 - 25- **Julian Dibbell:** A Rape in Cyberspace (or tinsociety, and How to make one), the village voice, Dec. 21, 1993.
 - 26- **Kittichaisaree, Kriangsack:** Public international law of cyberspace, Cham, Switzerland, Springer 2017.
 - 27- **Klaws W. Grewlich :** "Cyberspace": Sector-specific Relation and Competition Rules in European Telecommunication', Common Market Law Review VOL.36,(1999).

- 28- **Linda M. Harasim:** Global networks: an introduction, in Global Net works, 1993.
- 29- **Linda O. Simddy :** Choosing the law and forum for the litigations of disputes, in “toward a law of global communication networks” (Anne W. Branscomb ed. 1980).
- 30- **M.Colucci :** The Impact of the Internet., 2002, Kluwer.
- 31- **M.Laguerre :** The digital city , The American metropolis and information technology, 2005.
- 32- **M.R. Burnstein:** Conflict on the Net, choice of law in transnational cyberspace, Vanderbilt J. Trans. L., Vol. 29 Jan. 1996.
- 33- **Mark Eckenwiler:** Criminal Law and the Internet. Legal Times, Jan. 23. 1995.
- 34- **Markus Fallenböck:** Internet und Internationales privatrecht, zu den Internationalen Dimensionen des Rechts im Electronic Commerce, Wien, 2001.
- 35- **Masato Dogauchi:** Law applicable to Torts and copyright infringement through the internet., in Legal aspects of globalization (Jürgen Basedow and Toshiyuki Kono ed.) Kluwer 2000.
- 36- **Mattew R.Burnstein:** conflict on The Net, choice of Law in transnational cyberspace, vanderbeltj of trans L., vol. 22 , Jan., 1996, no1, p.80.
- 37- **Matthew Burnstein:** A global Network in compartmentalize legal Environment: in Internet which court syberspace? Which law applies?, K. Boele- Woelk (ed.) Kluwer, 1998.
- 38- **Michael Chertoff and Paul Roseenzweig :** A primer on Globally Harmonizing internet Jurisdiction and regulations, CIGI, Ontario, Canada, Global Commission on unilateral Governance, Proper Series : No. 10, March 2015.
- 39- Michael J. Sandel, America's search for a new public philosophy, Atlantic Monthly, Illustrations by Mirko Ilić, Mar. 1996.
- 40- **Monroexprice and stebaan G. Vohulst :** the concept of self – regulation and the internet, Univ. of Pennsylvania., scholarly commons, 2000.

- 41- **Nicola Lucchi** : Access to network services and protection of constitutional Right : recognizing the essential role of inter net access for the freedom of expression, Cardozo Journal of international and comparative Law, VOL. 19. No. 3/2011.
- 42- **P.K. Ohm**: On regulating the Internet: Use net, A case study, no. 46 U. California Law Review, 1999.
- 43- **Rosalind Resnick**: Cybertort: The New Era, National Law Journal, July 18, 1994, at A1.
- 44- **Stephan wilske**: International jurisdiction in Cyberspace: which stats may regulate the Internet?, Federal communications law Journal, Vol. 50, 1997. P. 117 Spec
- 45- **Trotter Hardy**, "The proper legal regime for cyberspace, University of Pittsburgh Law Review, Vol. 55, 1994, P. 993, Spec, in his Conclusion.
- 46- **Trotter Hardy**, The Proper Legal Regime For "Cyberspace", 55 University of Pittsburgh Law Review, 1994.
- 47- **Lawrence Lessig**, 'Reading the Constitution in Cyberspace', 45 Emory Law Review, January , 1995) 869- 910 spec., at 895-899.
- 48- **Stoll and Goller**, 'Electronic Commerce and the Internet', 41 GYIL (1998) 128.
- 49- **Lorna Gillies**, electronic commerce and international private law: A study of electronic consumer contacts, 2008.
- 50- **F. C. Mayer**, Europe and the Internet: the old world and the New medium, EJIL.11 (2000) .
- 51- **F.C. Mayer**, Recht und Cyber space. Eine Einführung in einige rechtliche aspects des Internet's. Humboldt Forum Recht 3 (1997) at IV,
- 52- **Margaret Loo**, IBM V. Commissioner: The Effect Test in the EEC, 10 Boston College, INT'L & COMP. L.REV. p. 125 (1987), Polished online by Cambridge University press. 21 July 2009;
- 53- **Dan.L. Burk**: Patents in Cyberspace: Territoriality and infringement on global computer, Tulane Law Rev. Vol. 68, Nov. 1993.
- 54- **Philip Adam Davis**, Indiana Univ., School of Law, The defamation of choice of Law in Cyberspace, Federal Communication Law Journal. Vol. 54, Issue 2, Article 6.