Preparatory Colloquium.
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

BRAZIL*

Fauzi Hassan CHOUKR[1] / Coriolano de Almeira CAMARGO[2]

(B). General Questions

(1) Are there current (legal or socio-legal) definitions for applications of IT and ICT (information and communication technology) within the context of criminal procedure (including forensics)? How are such conceptual definitions reflected in the literature, legislation, court decisions, and relevant practices within the context of the criminal process?

Brazilian Justices recognize the importance of increasing technological tools in order to provide a high quality of criminal justice system.

Indeed, in a suggestive work table on "Proofs and Information Administration: new paradigms" passed in 2010 the former STF Justice Chief Cesar Peluso has pointed that "the challenges are so many, but we have reasons to keep ourselves optimists. Judiciary branches walks to the dissemination of electronic process in all fields what means among other obvious advantages to incorporate in the criminal prosecution new shapes and types of proofs that we could not imagine in the "paper format" ".

Despite that optimism he concluded that the subject is polemic and must be respected all the defenders guarantees as well the efficiency of the system and put in relevance that this new model must be understood for all intervenient as judges, lawyers, prosecutors, police officers and workers of the legal justice system. At that point also the former Justice Secretary stressed the compatibility of the "new technologies" and defenders rights.[3]

The relevance of the theme speaks for itself and started to be heard during the 1990 decade after Brazil rebuilt the rule of law with the Constitution entered in force in 1988. At that time has begun a slow movement toward a new framework of criminal procedure, which original shape was established during the civil dictature in the years 1930/1940 conceived in a strict inquisitorial model. But that movement was known by the option that not changes criminal procedural Code as a hole, but slicing that law in their most important parts and modifying them.

In that way of (re)constructing criminal prosecuting system and taking in account what the technology offered at that time was tried the experience of "on line" defender's hearing[4] using an computer at the judge's room and another in the prison where the defender was arrested. That mechanism was strongly refused by Brazilian Courts when called to appreciate that "proof" in judicial review. The initiative was, then, abandoned.

That situation illustrates the aim to employ certain ground of technology in criminal prosecution but Brazilian law would not be changed until the 2000 decade as we will see below. As an instrument to stocking data the system will not be known relevant changing but after 2004 when was created the Nation Justice Council since then responsible for a new framework of administration in the Judiciary branches.

During the 2000 decade isolated experiences emerged in the practices of Brazilian criminal prosecuting system, mostly during the sentencing-executing phase.

One of them occurred in Rio Grande do Sul (South of Brazil) state in the year 2007 and intended to establishes an informatics parole's control specific dealing with the mandatory works of the convicted applied instead the prison penalty (so called SISCOPEN model).

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

1 Doutor e Mestre em Direito Processual Penal pela USP. Especializado em Direitos Humanos pela Universidade de Oxford e em Direito Processual Penal pela Universidade Castilla La Mancha. Professor do Programa de Mestrado/Doutorado da FADISP. Promotor de Justiça no Estado de São Paulo.

2 Lawyer, CEO of the Almeida Camargo Attorneys at Law, Teacher of the Pos-Graduation Program on Electronic Law and Cybernetics Intelligence at FADISP.

3 http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=167823 accessed in 05/04/2013.

4 GOMES, Luiz Flávio. O interrogatório a distância (on line). Boletim IBCCrim, São Paulo, n. 42, p. 6, jun. 1996.

Another initiative passed in Segipe state (northwest of Brazil) also related whith penalties control but target to keep an electronic data base of the sentenced benefits as ruled by Brazilian law nº 7.210/84 (Lei das Execuções Penais). Using the software inserted in the judge's computer one may control the period when the benefits will be served by the system as, for instance, the day when the sentenced will be transferred from the jail to the parole control. A similar system was introduced in 2010 at São Paulo state (southwest of Brazil) with the same goal. [5]

Trying change law and innovative practices were not enough to encourage the doctrine to increase the discussions on that subject and almost twenty years passed from the first attempt to apply technology in criminal prosecutions Brazilian literature on criminal procedure dedicates few pages to the information and communication technology and when she does so is to point the necessity to make compatible ICT with the defender's right. In this sense is more a conceptual discussion then about the mechanisms themselves. Actually, if one may try to understand that subject from the regular graduate literature used in Law Schools it´s possible not find one single word about that issue.

(2) Are there specific institutions and/or task forces involved in the implementation of ICT within the criminal justice system?

In 2004 was created by the 45a. Constitutional amendment both Nation Justice Council (CNJ) and National Prosecutor`s Council (CNMP) as "external" institutions in order to provide a social control on Judiciary and its branches and the Prosecutor branches as well.

Going beyond the original provisions and expectations, both controls were powered with another functions and became progressively strong mechanisms to change at the bottom the whole structure mostly the Judiciary one.

So, reports, studies, projects and new initiatives on justice system administration started to be applied and the use of information and technological resources to stockade data and cross them as well the access to the files register are being (slowly) introduced in all branches (civil, penal, labor and elections).

The mean initiative is "The Judicial Process Electronic (EO), computer system developed by CNJ in partnership with the courts for the automation of the Judiciary, was officially launched on 21 June 2011 by the Minister Cezar Peluso, president of the CNJ. The next day (22/06), Presidents of courts around the country attended a detailed presentation of the system and received a technical manual to assist in the installation of software. The event was broadcast live on the portal of the CNJ and had 1315 hits, and 135 concurrent. Furthermore, 32 courts relayed the presentation via streaming to their servers."[6]

As pointed, "The main goal is to maintain a CNJ lawsuit electronic system capable of permitting the practice of procedural acts by judges, servers and other participants in the proceedings directly against the system, and the monitoring of the judicial process, regardless of the process transact in court Federal Justice in the States, the States Military Justice and the Labor Court."

At last, "the EO also comes in an innovative criminal prosecution. Based on the observation that it is essential to aggregate information and individual information on crimes that affect the course of the criminal proceedings, was in CNJ specific group created to address the issue, involving magistrates and servers, as both the judicial area of information technology. As a result, features that are being developed by excel encompass the entire spectrum of criminal prosecution, the conduct of the inquiry into criminal rehabilitation, through the monitoring of criminal enforcement. Information in prison, release, sentencing are stored individually - by defendant - came to the detail to indicate the magistrates and servers which feathers are planned for each type criminal."

(3) Are there private (commercial) organizations (companies) that offer ICT related services to the criminal justice system? If so, can

you give examples? What limits have to be observed?

It's possible that official institutions buy software from private enterprises according Brazilian law once respected the law of publics contracts[7] that demands a previous competition among them as established by the general conditions on the edictal.

One of the most popular private information system used by the Judiciary and Prosecutor`s Office is the so called "SAJ" (Sistema de Automação da Justiça) or "Automation Justice System" employed by numerous institutions and developed by a private company[8] in order to provide easier access to data and to register a lot of working routines as well to make more accessible to the public obtain all information on judicial files still in course or even yet solved.

Despite that, must be stressed that great effort is being made by officials agencies to develop software without extra costs to all Judiciary branches even so Prosecutor`s Office or Public Defender`s institution.

---

5 Further information can be found in http://www.premioinnovare.com.br/

6 http://translate.google.com.br/translate?u=http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicial-eletronico-pje/a-gerencia-do-projeto&sl=pt&tl=en&hl=&ie=UTF-8

7 Law 8666, 21 june 1993.

8 http://www.softplan.com.br/saj/clientes.jsf

(C) Information and Intelligence: building information positions for law enforcement

(1) Which ICT-related techniques are used for building information positions for law enforcement agencies?

First of all is interesting to point the existence of the Law 9883, 07 December 1999 that reorganized the Brazilian intelligence system (SISBIN) and created the Brazilian Intelligence Agency (ABIN) as the mean organism. The same law also established the so-called "Sub-system of intelligence and public security" integrated by the analog institutions in the states (must be remembered the Brazilian federalist structure).

In the article 1, par. 2o provides that "must be understood as intelligence the activity that aims to obtain, analyze and disseminate the knowledge, inside and outside the country, about facts and situations of immediate or potential influence on decision make process and the governmental actions as well the integrity and safety of the society and the State".

Is necessary to put emphasizing that intelligence is not the same as investigation, but from the investigation emerges all sources to build an intelligence framework.

So, the techniques mostly employed to build a frame of information and intelligence are the surveillance of telecommunications (phone calls, SMS, e-mails and similar ones) and surveillance of live conversations at home or business places (audio but not video). Beyond that, financial registers in banking accounts in the country or abroad can be reached.

In all cases listed above is necessary a judicial order in the pre-trial phase or during the hearings before sentencing. Must be pointed that all that measures cannot be acted only for police initiative and the prosecutor's office in Brazil has no power to determinate that. Also must be stressed that all the information granted using the surveillance are linked with a specific case and cannot be stocked in order to constitute a data-base.

DNA data-base is a recent innovation in Brazilian law[9] and integrates the system of whole suspect's identification until them limited to fringe prints and biometrical information or photos recorded in specific books. Employed during the pre-trial phase, DNA identification is mandatory in case of conviction on heinous crimes or crimes using violence against a human being[10]

The same situation passed with DNA database, system created but not installed yet that was finally disciplined[11] and will put in progress using the CODIS (Combined DNA Index System).

(2) To which type of public (e.g. DNA databases) and private (e.g. PNR or financial data such as SWIFT data) databases do law enforcement agencies have access?

All agencies can access DNA, financial, bank or telecommunications data-base but only with judicial warrant not directly by police or intelligence forces or the prosecutor's office as well.

There is a great discussion in Brazilian case law about the possibility of prosecutor´s office or the Auditor's Court directly reach information existent in Brazilian Federal Revenue Office (BFRO) data-base. Some precedents authorize the direct request while the major position considers impossible to get access without judicial warrant[12] even the proper BRFO doing it directly to the banks[13].

(3) Can techniques labelled as data mining and data matching be applied? If so, can these techniques be used to create profiles of potential perpetrators or risk groups? If so, have special tools been developed for law enforcement agencies?

Data mining and data matching techniques could be applied mostly in intelligence field to construct profiles. But our literature, both academic[14] and case law don't have significant approach on that, what reflects the low use of that techniques by Brazilian police forces or federal/ states intelligence agencies.

Indeed, according a distinguished researcher on this subject, "rare are the Security Departments in Brazil where exist a specific branch for statistics and data colleting as well the technology for doing that. Federal government that makes a remarkable work on colleting data about economy, health or education has no structure to collect information related to crime. Only a few state police forces organized an informatics Operation Centre and modern data-center". Rarer are the those ones that contain an IT and mapping events and utilize that information in order to

9 Lei 12.654/2012

10 Art. 1o da Lei no 8.072, 25 july,1990

11 Decreto 7950, 12 march 2013.

12 About the Prosecutor´s Office see STJ, HC 160.646/SP, T5 - Quinta Turma, Rel. Min. Jorge Mussi, j. 01/09/2011, p. 19/09/2011; About the Auditor´s Court :MS 22801/DF (DJe de 14.3.2008). MS 22934/DF, rel. Min. Joaquim Barbosa, 17.4.2012. (MS-22934)

13 RE 389808/PR, rel. Min. Marco Aurélio, 15.12.2010. (RE-389808)

14 See as almost isolated paper in Brazilian criminal literature FERRO JÚNIOR, Celso Moreira; DANTAS, George Felipe de Lima. A descoberta e a análise de vínculos na complexidade da investigação criminal moderna. Jus Navigandi, Teresina, ano 12, n. 1441, 12 jun. 2007 . Disponível em: <http://jus.com.br/revista/texto/10002>. Acesso em: 16 abr. 2013.

provide planned operations".[15]

(4) Can coercive measures (e.g. interception of telecommunications) be used for building up information positions?

As explained before the fruits of surveillance of telecommunications can be used only for the specific case (investigation; trial), which they were allowed. And, the same way with DNA information.

This is a consequence of Brazilian legal model that imposes those measures only under strict judicial control and for a straight use. In this sense cannot be conceived – according the legal framework – general warrants to interception telecommunications without a deadline. [16]

Despite that legal provision there are often suspicious of illegal interceptions mostly in federal or states prisons that would occur without judicial warrants and not linked to a regular investigation or trial

(5) Which private actors (e.g. internet providers or telecom companies) retain or are obliged to retain information for law enforcement agencies?

Commercial transactions in Brazil, as a general rule, generate an invoice / purchase and that document must be kept during five years from de date when issued by the responsible of the transaction and, when requested, must be delivery to the authorities. In a large range of situations there is no necessity of a judicial warrant, unless the document must be employed against the person that keep it.

About the telephonic communications all enterprises that furnish this kind of product must keep in their servers records the CDR's (Call Detail Record) or IPDR's (VoIP Detail Record) for, at least, five years.

Must be pointed that CNJ has issued the Resolution 59, 09 September 2008 which rules the way the judges must address the judicial order to the companies when determine to disclosure telecommunication information. In this particular subject is discussed even if the data furnished when a cell phone plan was celebrate (e.g. name, address) must be delivered only under judicial warrant. Significant doctrine[17] appoints to the possibility of free access without judge's intervention in that situation.

About Internet, Brazil discuss at present time the regulatory law[18] and in its article 10, par. 1o., is mentioned that all the information contained in the provider only can be disclosed through a judicial warrant[19]. In the following article there is a rule that commands the provider to keep all the connections records for one year[20]. There no prevision when this law will enter in force and there are serious discussion on that opposing the draft law against intimacy and privacy rights.[21]

At end is important to clarify that in Brazil all this matter is ruled by federal law (despite our federative structure) and beneath that there are normative rules issued by the mean regulatory agency denominated ANATEL (Agência Nacional de Telecomunicações or Telecommunications National Agency).

That is a relevant point because are knew some attempts made by the states in order to rule the delivery of data inserted in telecommunications enterprises to prosecutor's or investigator's forces. This has passed at Rondonia State (North of Brazil) that made entered in force the Law 2659/11 that provided the obligation of that enterprises to disclose to the authorities the information about the exact place were a cell phone was in a certain period. The law

15 BEATO FILHO, C. C. . Informação e Desempenho Policial. Teoria & Sociedade (UFMG), Belo Horizonte / UFMG, v. 7, p. 117-150, 2001

16 About deadline see the following precedent: A Lei n. 9.296/1996, que regula a quebra de sigilo das comunicações telefônicas, estabelece em 15 dias o prazo para duração da interceptação, porém não estipula termo inicial para cumprimento da ordem judicial. No caso, a captação das comunicações via telefone iniciou-se pouco mais de três meses após o deferimento, pois houve greve da Polícia Federal no período, o que interrompeu as investigações. A Turma entendeu que não pode haver delonga injustificada para o começo da efetiva interceptação e deve-se atentar sempre para o princípio da proporcionalidade, mas, na hipótese, sendo a greve evento que foge ao controle direto dos órgãos estatais, não houve violação do mencionado princípio. Assim, a alegação de ilegalidade das provas produzidas, por terem sido obtidas após o prazo de 15 dias, não tem fundamento, uma vez que o prazo é contado a partir do dia em que se iniciou a escuta, e não da data da decisão judicial que a autorizou. Precedente citado: HC 135.771-PE, DJe 24/8/2011. HC 113.477-DF, Rel. Min. Maria Thereza de Assis Moura, julgado em 20/3/2012.

17 FERRAZ JUNIOR, Tercio Sampaio. Sigilo de Dados: o Direito à Privacidade e os Limites à Função Fiscalizadora do Estado. In Sigilo Fiscal e Bancário. PIZOLIO, Reinaldo e GAVALDÃO JR, Jayr Viégas (coord.). São Paulo. Quartier Latin. 2005. p. 28-29

18 Draft Law 2.126, DE 2011.

19 Art. 10. … § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo.

20 Art. 11. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.

21 E.g., http://www.senado.gov.br/noticias/senadonamidia/noticia.asp?n=590252&t=1

was refused by the Supreme Court considered its unconstitutionality. [22]

(6) Which private actors can provide or are obliged to provide information to law enforcement agencies?

As clarified above, both enterprises and public agencies must provide information when requested through a judicial warrant or when directly requested by the prosecutor or investigator's forces. Must be remembered that in the first hypothesis (judicial warrant) privacy or intimacy play a significant role and in the second situation there is no risk to that fundamental right.

Anyway, in case of unjustifiable refuse of that order (with or without judicial warrant) to provide information the person concerned (only natural ones) may be prosecuted for committing a felony of attempt of court.

(7) Is there judicial control on building information positions?

Judicial control exists only in the specific case which the warrant to provide information was issued.

For example, Brazilian law on telecommunication interception and CNJ normative quoted above determine that the police force that is in charge of the surveillance or interception must report after a certain period all the fruits of that investigation technique.

But, as already stressed, those information are limited to the case and cannot be used to construct a whole framework of data. The exception to that rule can be observed when during a regular telecommunication interception polices forces discover information about another crime. But this example cannot be understood as a real building information network.

(D) ICT in the criminal investigation

(1) Can law enforcement agencies carry out interception in real time of a) e-traffic data; b) content data?

Brazilian law admits the real time interception ruled as above mentioned through a judicial warrant and since 2011 a system called Sistema de Interceptação de Sinais (SIS) can be played by the police forces under judicial supervision as well the Prosecutor's Office and the CNJ. This model makes unnecessary the intervention of telecommunications enterprises once the interception is made using a proper software developed by Anatel, CNJ and General Prosecutor's Office. The former device employed by police forces was "the guardian" that can, simultaneously, intercept 5.000 phone calls

(2) Can law enforcement agencies have access to/freeze/search/seize information systems for a) e-traffic data; b) content data?

This kind of technique can be played, but only with judicial warrant using the same logic and law basis as telecommunications nterception.

(3) Can telecom companies or service providers be obliged to share data with law enforcement agencies? In case of noncompliance,

are there any coercive measures or sanctions?

There is no obligation to share information e.g. when a cell plan is sold or when a SMS is sent. The only obligation is to keep certain data as ruled by federal law or ANATEL provisions that must be delivery to the enforcement agencies when requested by a judicial warrant.

(4) May law enforcement agencies apply video surveillance? Can they oblige natural or legal persons to cooperate?

There is no specific provision in Brazilian law about video surveillance used by police forces, but some of them use cameras inside official vehicles mostly when in course investigative measures aiming to avoid police abuse, system that works not so well for that goal[23].

But in some Brazilian cities is growing a slow movement to implant video cameras all around the perimeter or at least in the mean pointing that are.

In that case the system is handled or by municipal police (that have no powers to investigate or prosecute in Brazil) when he can be shared with the other police forces[24] or by military police (police forces that, in Brazil, is in charge for the ostensive police surveillance).

For illustrate the video surveillance handled by military police can be told the experience occurred in Santa Catarina State (South of Brazil) in the cities of Joinville and Florianópolis (respectively the greatest city and the capital of that State) where since 2001 was implanted a video surveillance system with cameras insert in top in public places points

22 ADI 4739 MC/DF, rel. Min. Marco Aurélio, 7.2.2013. (ADI-4739)

23 See the following experience occured in Ceara state (Northwest of Brazil): http://www.tribunadoceara.com.br/noticias/video/apesar-de-monitoramento-por-cameras-policias-cometem-abusos-no-trabalho/

24 See the following experience in Jundiaí city (São Paulo State; southwest of Brazil): http://www.segurancaeletronica.org.br/noticia.php?not=114

connected by optical wires and played twenty-four hours seven days by seven.[25]

Beyond that, police forces can ask for tapings made for private or public surveillances (e.g. bus station, banks, streets) in a specific investigation.

(5) May or must law enforcement agencies apply audio-visual recording of interrogations (suspects, witnesses)?

There are no specific rules about that and this initiative depends of isolated agents when interrogating a suspect. However there is a draft law[26] specific about this issue disposing that " [police authority] … must hear the suspect…and recording the interrogatory in audio and video …".

Must be added that the recording of an informal conversation between the suspects and police forces during the transportation of that person to the police station cannot used against him unless he has advertised that could be used in the Court if necessary[27]

(E) ICT and evidence (The chain of stages: collecting/storing/retaining/producing/presenting/evaluating electronic evidence)

(1) Are there any rules on evidence that are specific for ICT-related information?

Brazilian law does not provide specific rules on ICT proofs. The recent Law 12.737, 30 November 2012 that entered in force four months later and only deals with penal provisions as cyber-crimes but no possess procedural provisions.

For that reason all rules about e-proofs are interpreted as a following of the general rules on proof contained in the procedural penal code established in 1941 what demands a lot of problems of compatibility and specificity. Actually this subject is broader discussed by the civil procedural doctrine as the penal one[28]

(2) Are there any rules on integrity (e.g. tampering with or improper processing) and security (e.g. hacking) of ICT-related evidence?

There are no specific provisions on integrity or security of ICT but a general rule that came from the Brazilian model of ICP-Brazil is the bases of the subject once this systems provides the assurance of integrity of the documents an all virtual transactions.

About DNA proof in criminal field must be pointed the general rules for obtaining and keeping material as ruled by the National Network of Forensics Genetic following the general instructions issued by the São Paulo Security Department (Rule. 194 - SSP/SP)[29]

(3) Are there any rules on admissibility (incl. the principle of procedural legality) of evidence that are specific for ICT-related information?

(4) Are there any specific rules on discovery and disclosure for ICT-related evidence?

(5) Are there any special rules for evaluating (probative value) ICT-related evidence?

Brazil has no specific provisions on admissibility of ICT or related proofs/ information and as well about discovery or disclosure ones.

For that reason, as explained before, all general rules of CPP and, above all, Constitution and Interamerican Convention on Human Rights must be applied. In this sense all discussion that could be in that matter are potentially the same as already noticed on illegal proofs and exclusionary rules.

The same ground of analysis must be applied on evaluating evidence coming from ICT or related information by the judge.

In despite the fact that there is no preponderance of technological proofs in comparison whit the others in the legal framework, some of ICT or related proofs are naturally put in a stage above as telecommunications interceptions or

25 http://revista.ssp.go.gov.br/index.php/rebesp/article/viewFile/72/27

26 PL 3852/2012 in course in the House of Representatives.

27 The following precedent: É ilícita a gravação de conversa informal entre os policiais e o conduzido ocorrida quando da lavratura do auto de prisão em flagrante, se não houver prévia comunicação do direito de permanecer em silêncio. O direito de o indiciado permanecer em silêncio, na fase policial, não pode ser relativizado em função do dever-poder do Estado de exercer a investigação criminal. Ainda que formalmente seja consignado, no auto de prisão em flagrante, que o indiciado exerceu o direito de permanecer calado, evidencia ofensa ao direito constitucionalmente assegurado (art. 5º, LXIII) se não lhe foi avisada previamente, por ocasião de diálogo gravado com os policiais, a existência desse direito. HC 244.977-SC, Rel. Min. Sebastião Reis Júnior, julgado em 25/9/2012.

28 See among others references: BLUM, Renato O. A Internet e os Tribunais. In: REINALDO FILHO, Demócrito (coord). Direito da Informática: Temas polêmicos. Bauru, SP: Edipro, 2002; LESSA, Breno Munici. (03/2010) A invalidade das provas digitais no processo judiciário. http://jus.uol.com.br/revista/texto/14555/a-invalidade-das-provas-digitais-no-processo-judiciario/print . Acesso em: 03/11/2010; PINHEIRO, Patrícia P. Direito Digital. 3. Ed. São Paulo: Saraiva, 2009

29 http://www.mj.gov.br/senasp/SUSP/pericias/pericia_dna.htm

DNA tests. [30]

(F) ICT in the trial stage

(1) How can or must ICT related evidence be introduced in the trial?

Brazilian penal procedure establishes that the evidence must be requested by the prosecutor in the indictment act that is wrote and addressed to the judge even in the case of trial by jury. The defense counselor presents its proofs ordinarily when the preliminary defense that is also wrote and addressed to the judge.

In the ordinary proceeding is conceived a single hearing session when the victims, witnesses, experts and defend must be heard. Despite that provision this whole hearing rarely is coming true in practice mostly for operational reasons.

As a rule ICT proofs are obtained by the prosecutor during the pre-trial phase when the defender can no interference and only can be discusses after the chargers were accepted and presented in trial. By the defense those proofs are mostly requested, produced and presented during the trial.

(2) Can distant interrogations (e.g. by satellite connections) be applied?

After a great discussion started in 1990 years as quoted above, Brazilian legal system adopted Law 11900, 8 January 2009 that contains all regulation for videoconference interrogations as well the hearings of victims and witness.

However there is strong controversy on that subject with a great number of scholars considering that law unconstitutional once there are offenses to defenders rights, position that account with no unanimity[31] .

Despite that there is no unconstitutional declaration on that law by the Supreme Court and all the governments stresses the support on that measure[32] including as a tool do became the judicial system less expansive

(3) Can digital and virtual techniques be used for the reconstruction of events (killings, traffic accidents)?

There is no objection on that initiative on Brazilian law but there is no official software that could be used what means, in practice, that the player that wants to make use of that mechanism will suffer the opposition of the other part not for a problem of admissibility but the reliability of the measure.

(4) Can audio-visual techniques be used to present evidence at trial (in its simplest form: pictures and sound)?

In that case there is no objection on that initiative according Brazilian law. But there is a particularity in the trial by jury what means in Brazilian procedural system only murder cases and that imposes the notification of the "ex adverso" about the showing of the video or pictures at least tree days before the hearing. Brazilian system admits no surprises during the statements.

(5) Can criminal "paper" case files be replaced by "electronic ones"? Are there any developments towards digitalizing of the trial proceedings

Introducing a digitalized file model is the contemporary struggle of CNJ[33] and almost all Courts in Brazil as well the General Prosecutor´s Office as consequence of Brazilian Law 11419, 19 December 2006 that created the legal basis for the digital process.

In the criminal field there is a significant obstacle because the greatest part of the investigation is ruled by the police itself and there is no equivalent initiative in the police forces to digitalize the pretrial files.

30 Specific about DNA tests and its repercution on brazilian case law see http://www.mackenzie.br/fileadmin/Graduacao/FDir/Artigos_2008/Marco_Antonio_de_Barros_2.pdf

31 ARAS, Vladimir. O teleinterrogatório não elimina nenhuma garantia processual. In: Consultor Jurídico, São Paulo, 28/09/2004 [Internet]. Disponível em: http://www.conjur.com.br/2004-set-28/teleinterrogatorio_nao_elimina_nenhuma_garantia processual; GOMES, Rodrigo Carneiro. Videoconferência: tecnologia a serviço da sociedade. Revista Consultor Jurídico, São Paulo, SP, 08 jun. 2009. Disponível em: http://www.conjur.com.br/2009-jun-08/videoconferencia-tecnologia-servico-sociedade-bem-publico..

32 TJSP e governo de São Paulo assinam termo para ampliar sistema de videoconferência. In: Conselho Nacional de Justiça, Brasília-DF, [Internet]. Disponível em:http://www.cnj.jus.br/index.php?option=com_content&view=article&id=7135&Itemid=675.

33 See **https://projudi.tjmg.jus.br/projudi/** as an example of that initiative that occurs in all country.