Geraldo Prado

MA and PhD in Law. Post doctoral fellowship in the History of Legal Ideas and Culture from the University of Coimbra. Professor of Criminal Procedural Law at UFRJ.

Producing criminal evidence and new technologies: The Brazilian case[1]

Delineating the problem

1. The main theme of the Seminar, "Interactions between Law and Internet", refers to a dense and diversified set of relationships tying legal knowledge (and its practical applications) to new communication and information technologies, to be examined from the angle of the worldwide web (Internet).

2. The decision to demarcate a specific space for internet-related issues allows for a deeper analysis on internet controversies in which a meticulous analysis is necessary; such controversies typically involve nuances that are not always visible within the totality of situations involving the use of digital technology in the legal field. This is why an expressive contingency of cases affecting the so-called "electronic process", which only eventually have direct involvement in the topic proposed at this table, have been deliberately left out of the analysis.

3. The use of electronic means for court cases in Brazil is regulated by Lawº 11.419, from December 19, 2006[2], but the law does not focus on those questions concerning evidence, except for the digital documentation method

[1] Speech given on June 7, 2013 for the seminar "Interações Direito e Internet" (Interaction between Law and Internet), in São Paulo, promoted by the Lawyer's Association of Sao Paulo (AASP), receiving support from Google Brazil and the Association of Federal Judges (AJUFE).
[2] http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm Consulted on May 31, 2013. On the electronic process in Brazil: ALMEIDA FILHO, José Carlos de Araújo. Processo eletrônico e teoria geral do processo eletrônico: a informatização judicial no Brasil, 4ª ed. Rio de Janeiro, GEN/Forense, 2011.

used in procedural acts, including approbatory content. Law nº 11.419/06 applies to criminal cases, yet as far as this presentation is concerned, the weight of such cases is quite relative and this approach is only justifiable in an incidental way.

4. This intervention is centered on the relationship between criminal proof and new communication and information technologies, in their ties to the worldwide web, a problem sufficient enough to aggregate a serious amount of issues interpolating law as well as other fields of knowledge and that demand from those involved in solving legal problems the temporary suspension of certain concepts and beliefs consolidated over decades of working experience in the legal field.

5. With the aim of extracting as much as possible from the debate the perimeter of controversies will be even more restricted to looking at the flow of internet-based data as a source of evidence or a means of obtaining proof in criminal cases[3].

6. What should be inquired in other words: does Brazilian law authorize intercepting and apprehending email from the web and/or employing it, stored in databases, in order to influence criminal investigations and/or criminal cases?

7. In addition, it's worth considering the role played by private enterprises, such as internet email provider services, keeping in mind the generalized and consensual recognition of communication privacy as a fundamental right.

[3] Reference will only be made to Brazilian criminal law in an incidental way within this scope. It's revealing to note, however, that on November 30, 2012 Law nº 12.737 was edited. This law concerns punishing conduct defined as informational violations (arts. 154-A, 266 and 298 of the Brazilian Criminal Code).

www.geraldoprado.com

8. Hence, problems originating in the criminal procedural use of data taken from email and the transnational character of email activity itself may be summed up to the previous question. As such it's a relevant part of this hypothesis to also interrogate the pertinent legal regime and the limits of internet providers' responsibilities[4].

A preview

9. The questions proposed here deal with the delicate tension between individual rights and the common good, touching the heart of public freedom (of expression, communication, informational freedom, etc.).

10. This motion leaves no space for "easy answers", in spite of strong temptations to look for them, for example, by invoking the limits of individual rights when there is a risk to public safety and by thus indentifying points of contact or symmetry between dangers to public security and establishing the responsibility of those suspected of practicing crimes.

11. Evidently this doesn't mean exclusively interpolating Brazilian legal doctrines and courts. To the contrary, the wealthy bibliography on this subject and on convoking supranational paradigms in order to inspire diverse solutions adopted in other countries reveals how complex and tormenting this problem is[5].

---

[4] Basically on internet provider services: ZANIOLO, Pedro Augusto. Crimes modernos: o impacto da tecnologia no Direito, 2ª ed., Curitiba, Juruá, 2012.

[5] Merely as an illustration: LUPÁRIA, Luca *et alli*. Internet provider e giustizia penale: modelli di responsabilità e forme de collaborazione processuale, Giuffrè, Milano, 2012; RIVES SEVA, Antonio Pablo. La intervención de las comunicaciones en el proceso penal: análisis doctrinal, legislación y jurisprudencia, Barcelona, Bosch, 2010; ARMAZA, Emilio José Armaza (coord.). La adaptación del derecho penal al desarrollo social y tecnológico, Comares, Granada, 2010; RODRIGUES, Benjamim Silva. A monitorização dos fluxos informacionais e comunicacionais: contributo para a superação do "paradigma da ponderação constitucional e legalmente codificado" em matéria de escutas telefónicas, vol. 1, Coimbra, 2009; JASANOFF, Sheila. Science at the Bar: Law, Science and Technology in America, Harvard University Press, 1995; LANDAU, Susan. Surveillance or Security? The Risks Posed by New Wiretapping Technologies. Cambridge, MIT Press, 2010.

12. The worldwide situation, especially after 9/11, the Madrid attacks, and March 11, 2004 elevated the tension and “stress” level in terms of controlling the circulation of people and information, characteristic of this new moment of global society. The transnational diffusion of feelings of generalized insecurity incentivized punctual paradigmatic changes that reflected on criminal practices. Pilar Calveiro rightfully alludes to general procedures that established new modalities of penalization and punishment in the local as well as international realm[6] as a direct result of this perception.

13. Ulrich Beck warns that this common-sense “cultural perception of risk”, distinct from risk itself, as an “anticipated event” understood in a rational way[7]. Currently people are accustomed to living with what has been become known as “risk subjectivity”. Communication technologies, “interconnecting the world”, contribute to this sensation, configuring an instrument through which symbolic ties are woven locating everyone for the first time in history in a “common present”[8].

14. In different ways both Pilar Calveiro and Lorena B. Winter highlight that the “risk economy” channels tensions in the clash between seeking safety, on the one hand, and protecting fundamental rights on the other[9].

---

[6] CALVEIRO, Pilar. Violencias de Estado: la guerra antiterrorista y la guerra contra el crimen como medios de control global. Buenos Aires, Siglo Veintiuno, 2012, p. 12.

[7] BECK, Ulrich. La sociedad del riesgo mundial: en busca de la seguridad perdida. Barcelona, Paidós, 2008, p. 30.

[8] *Idem*, p. 31. Manuel Castells, in his preface to the 2010 edition of “A sociedade em rede” (Rio de Janeiro, Paz e Terra), affirms that “we live in confusing times”, marked by “a process of multidimensional and structural change occurring in the midst of agony and uncertainty”. Castells adds that “the sensation of disorientation is formed by radical changes in the communicational environment, derived from the technological revolution in this field” (quoted work, p. I).

[9] WINTER, Lorena Bachmaier. Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos, **in** 2º Congresso de Investigação Criminal, coord.. Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes. Coimbra, Almedina, 2010, p. 162.

15. As the legal field, and especially criminal law, were called onto the scene, these have reacted by coming up with strategies in order to control criminality and have exercised power in such a way as to frequently interpolate public freedom and affect personal privacy.

16. By looking at the Portuguese and German experiences, Manuel da Costa Andrade warns that the new procedural reality contemplating figures "*particularly invasive and investigated in an unequal fashion"*, characterized by "*secret means*", has also demanded that the doctrine "*reinforce the potential for guarantees*"[10].

17. In general, telephone and worldwide web communications have become the protagonists of such "secret means" that challenge the legal order to institute the normative limits between valid and invalid, licit and illicit, within a context of respecting the rules of democracy which are being permanently tested in an environment of generalized mistrust and in the dominion or manipulation of a diffuse feeling of insecurity ("subjective risk", as Ulrich Beck would say).

18. The first step towards instituting clear borderlines in the legal order is by maintaining this topic within the realm of the Law, in conformation with the constitutional paradigm and in reverence to the treatment given to such material by international human-rights treaties.[11]

[10] COSTA ANDRADE, Manuel. "Bruscamente no verão passado", a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra, 2009, p. 21. The author points out that, if in 2004 the German Federal Constitutional Court knew how to restrain the operation known as the "great inquiry" (*grosse Lauschangriff*), because of the dense and profound decisions taken in light of this new procedural reality, figures "*of investigation particularly invasive and unequal"*, characterized by the so-designated "*secret means*", have also demanded that the doctrine "*reinforce the potential of guarantee*.

[11] In Germany, for example, the law on telecommunications surveillance was submitted to criteria of suitability extracted from the agreement reached at the Federal Constitutional Court on March 3, 2004, inspired in criteria of human rights tutelage extracted from the European Convention of Human Rights (ECHR), according to the interpretation of the European Court of Human Rights (ECHR). Vide: ROGALL,

www.geraldoprado.com

19. Therefore, constitutionally protecting communications makes it necessary for the Brazilian legislator, in order to regulate exceptional cases of violating communications privacy, the so-called "proportional reservation". This would explain the decision made by the Federal Supreme Court not to reception the point of the Brazilian Telecommunications Code of Law[12] and open a court procedure in order to edit the current law regulating telephone-call interceptions.

20. In Brazil, the legal regime for intervening in communications is disciplined by the dispositions of art. 5, inc. XII, of the Federal Constitution[13], regulated by Federal Law nº 9.296/96[14].

21. The current Criminal Procedural Code (CPP) doesn't give any special focus to this issue, comprehensible since its structure was inherited from the original 1941 model, when such topics simply weren't an issue at all. Later manifestations, even those recently altering the legal statute of proof[15], didn't substantially change the structure conceived during the Vargas dictatorship. As such, the distinct concepts of sources and means of proof continue promiscuously living side by side in the the Code of Law regulating Brazilian criminal procedure.

22. In the same way, the general regime of legal relationships with foreign authorities has not been updated by the Code (CPP) and the legal treatment given to the so-called "direct assistance" is the result of multilateral and

---

Klaus. A nova regulamentação da vigilância das telecomunicações na Alemanha, **in**: 2º Congresso de Investigação Criminal. Coimbra: Almedina, 2010, p. 118.

[12] On the proportional reservation of law, protection of communications, and the context of the advent of Law nº 9.296/96: PRADO, Geraldo. Limite às interpretações telefônicas e a Jurisprudência do Superior Tribunal de Justiça, 2ª ed., Rio de Janeiro, Lumen Juris, 2006, especially items 19-24 and 48.

[13] "The secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts" http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/constituicao_ingles_3ed2010.pdf

[14] http://www.planalto.gov.br/ccivil_03/leis/l9296.htm Consulted on May 31, 2013.

[15] Law nº 11.690, of June 9, 2008. http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm Consulted on May 31, 2013.

bilateral international legal agreements that have rarely been targeted for a more meticulous analysis on the part of specialized lawyers in this field[16].

23. A proposal for systematic legislative updating is contained within the Criminal Procedural Code project, currently being analyzed in congress[17]. Basically, the project contemplates a distinction between means of proof and means of obtaining proof and regulates intercepting the flow of communications in informational and telephonic systems (art. 246, § 3, inc. I), as well as “other forms of communication transmitted by data, signals, sounds, or images” (art. 246, § 3, inc. II), that are now considered as means of obtaining proof.

24. In addition, the project timidly establishes rules for executing interception orders on the part of communication provider services (art. 253 §§ 1 and 2 and 254, §§ 1 and 2), and, finally, directs assistance to the sphere of International Legal Cooperation (art. 694, § 1), with a view towards more adequate regulation (art. 695/9, 713/5 and 726/30).

25. Future legislative programs presume as irrefutable the hypothesis of legal validity of intercepting emails; this “common place” is an *a priori* of decisions taken by Brazilian courts that mandate the interception of electronic messages and apprehension of data, and also gather private information from internet provider services.

26. The hypothesis sustaining these decisions, however, consists in questioning the interception of emails as a method of access to sources of proof,

---

[16] For more on this subject: Manual de Cooperação Jurídica Internacional e Recuperação de Ativos do Ministério da Justiça (National Justice Secretary), Brasília, 2008. In the legal literature: BECHARA, Fábio Ramazzini. Cooperação jurídica internacional em matéria penal: eficácia da prova produzida no exterior. São Paulo, Saraiva, 2011.

[17] PL 8.045/10. http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

i.e., as a means of obtaining proof. I don't believe this is possible since it's not possible to intercept correspondence by using a physical support.

27. The problematic context quoted above makes it inevitable that the legal internet provider regime needs to be called into question, since the service itself is responsible for guaranteeing internet communication privacy. After all, electronic and traditional mail services are almost intuitively seen as equivalent[18].

28. As such, before even starting to probe into means and modes of executing interception orders for emails, the following question should be asked: may constitutional support be found for such interception?

29. At this moment "preventative interception" is not being cogitated in order to avoid that serious crimes be committed, but it should be emphasized right from the start that admitting the hypothesis of "preventative interception", in my point of view, is only valid if it is regulated by law, so as to guarantee the due court process and the aforementioned proportional reservation. In this regard it's worth recalling the decision made by the European Court of Human Rights (ECHR) in the case *Jalloh v. Germany*, on July 11, 2006, declaring that "even in the most difficult of circumstances, such as the fight against terrorism or organized crime, protecting human rights may not be negotiated beyond the limits and exceptions contemplated in the European Convention of Human Rights"[19].

---

[18] The legal statute governing relationships between an internet provider managing email services and the user of these services is complex: on the one hand are problems peculiar to private law regarding the quality of the services provided and complying with contractual obligations that link the two parties; on the other, the provider itself is submitted to public law, of constitutional origin, which takes into consideration its duties of maintaining privacy that the *resource itself*, i.e., the email service, must preserve.

[19] WINTER, Lorena Bachmaier. Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos, quoted on p. 163.

A problem ignored is still a problem

30. Effectively, admitting the hypothesis of intercepting email as *data*, i.e., without questioning such interception as a problem, but making it a premise, as is the case in the Brazilian legal order; namely, authorization to intercept messages transmitted by electronic mail (previous understanding of the situation at hand).

31. Other *data* incorporated naturally into the argumentation claims legal permission to investigate serious illicit crimes such as, for example, drug trafficking and corruption, aiding authorities by using secret invasive means of investigating informative elements.

32. Such reasoning is structured around a combination of two premises recognizing that serious delinquency thrives on new and efficient communication and information technology in order to carry out crimes. A similar hypothesis supposes the criminal repression should equally resort to sophisticated means of observing and gathering information.

33. This has been the tonic of most Brazilian criminal processes and almost always rises above the objection that the Constitution[20] doesn't authorize intercepting data, except for telephone calls, under the argument that it's possible to interpret the constitutional precept, which thus creates exceptions allowing for the hypothesis of intercepting telephone and other forms of communication data, putting them on par with each other. This premise is that what

---

"Even in the most difficult circumstances, such as the fight against terrorism and organized crime the protection of fundamental rights remains non-negotiable beyond the exceptions and derogations provide by the Convention itself".

[20] Aforementioned inc. XII of art. 5 (see note 13).

permitting data interception may be given legal backing by the single paragraph of article. 1º of Law nº 9.296/96[21].

34. I don't agree with this interpretation. The truth is that simply not dealing with the problem of inexistent constitutional permission to intercept email reveals how criminal procedural practices in Brazil still persist from the times of authoritarian regimes from which key criminal laws were framed and that, in each respective regime, framed Brazil as part of the scenario of communities under authoritarian traditions.[22]

35. The rupture with the authoritarian past, formalized in the creation of the 1988 Federal Constitution, among other consequences, affiliated Brazil to "the community of democratic traditions" of criminal procedures, whose stepping stone is the presumption of innocence and the premise consists in conceiving criminal procedure as an instrument of contention of public punitive

---

[21] "Single Paragraph. This Law applies to intercepting the flow of communications in informatics and telematics systems." Afterwards, the National Justice Council (CNJ), organ responsible for external control of Brazilian legal powers edited Resolution nº 59, from September 9, 2008, with the aim of standardizing routines for intercepting telephone, informational, and telematics systems. This resolution was struck down by the Federal General Attorney using the Ação Direta de Inconstitucionalidade (ADIN 4145). It's revealing to note that there has been no direct questioning of the ADIN regarding the unconstitutionality of regulation - in theory - on intercepting data since this would offend the inviolability of this kind of communication. This act was created on the basis of inadequate resolution, *and not the law itself,* in order to deal with issues that, in restricting individual rights, raise the need for the *previous law*. The ADIN also invests against the lack of competence of the CNJ to make decisions on this issue, this being the fundamental point of the controversy.

[22] Date of the Vargas dictatorship period (1937-1945), when the Criminal Procedural Code was edited, the "founding myths" of the Brazilian procedural code were consolidated and diffused, such as the "search for real truth", that justified intense probative acts by judges, instead of by the parts, an inquisitorial trait still found to this day in Brazilian criminal practice. The clearly authoritarian posture of the Justice Minister Francisco Campos, an organic intellectual in the Vargas regime and one of the signers of the Exposition of Motives of the Criminal Procedural Code of 1941, was revealed in the preferential option for the supposed "tutelage of the common good", inspired in fascism in detriment of individual rights. Marilena Chauí (Brasil: Mito fundador e sociedade autoritária. São Paulo, Perseu Abramo, 2000, p. 9) warns about one of these (ideological) traits of the founding myths: "this myth imposes an internal tie to the past as origin, i.e., with a past that never ends, that is permanently present and, as such, doesn't allow differential time and understanding the present time as such". Brazilian criminal procedure is competently dealt with by Rubens Casara in "Mitologia Processual Penal" (São Paulo, Saraiva, to be published), his PhD dissertation.

powers, as stated in the Constitution and, principally in international human rights treaties.

36. Hence the challenge of renewing the constitutional interpretation regarding Brazilian criminal procedural law and transforming its modus operandi. In both cases very little of the heritage of the legal-procedural categories consolidated from 1940-1980 have survived and the "meanings" shared during this period span regarding key concepts, such as presumption of innocence, a due legal process, the role of the criminal judge, the accusatory principal, etc., should now be reread.

37. Brazil's entrance into the community of democratic traditions and the accumulated product of "authoritarian modes of thought" call for seeking within democratic communities, with whom the country maintains historical ties - and that have gone through a democratic transition in the Twentieth Century – some of the bases for reconstituting the aforementioned key concepts. Otherwise these key concepts will continue to be guided by Brazilian constitutional interpretation, in a phenomenon defined by José Carlos Barbosa Moreira and Luis Roberto Barroso as "ordinarization of the Constitution" meaning submission to the parameters of the interpretation originating in the preceding common law.

38. Therefore understanding eventual conflicts between individual and communitarian interest is not an issue, as Francisco Campos has claimed, in his Exposure of Motives of the Criminal Procedural Code, in terms of abolishing "the unjustifiable primacy of individual interest over social tutelage"[23]. In the clash quoted above, the equivalent opposition, in terms of contemporary philosophy, was developed as part of the controversy "communitarian" versus

[23] Item II of the Exposition of Motives of the Criminal Procedural Code (September 8, 1941).

www.geraldoprado.com

"liberalism, but the term *community*, as employed in the discussion, "is primordially a democratic and participative meaning", as Rainer Forst cautions[24].

39. To say "common good" doesn't necessarily mean affirming something contrary or hostile to "individual interests".

Criteria for interpretation among communities with democratic traditions

40. The rapid evolution of communication and information technologies and the dialectic tension between public freedom, that the inviolability of communications protects, and the security of legal goods under the tutelage of criminal law, at first provoked perplexity and hesitation.

41. Even though computer networks have been around for a while, it was when the internet became a popular tool, in the early 1990s in Brazil, and in the 1980s in the USA, with the diffusion of more sophisticated methods of using this kind of technology, that the web came onto the crime "radar" and became a means of planning and carrying out crimes. And, naturally, as a result, internet technology also turned into an important source of legal proof[25].

42. Initially, the dialectic tension took as a critical point technique. After all, weren't/aren't the telematics or electronic mail flow instantaneous, and, just like telecommunications technology, don't leave behind any traces?

43. The term "*data*", meaning a digital representation of information was too abstract to guarantee a wide consensus in the legal field on the

[24] FORST, Rainer. Contextos da Justiça. São Paulo, Boitempo, 2010, p.11.
[25] For a panoramic vision: RODRIGUES, Benjamim Silva. A monitorização dos fluxos informacionais e comunicacionais: contributo para a Superação do "Paradigma da Ponderação Constitucional e Legalmente Codificado" em Matéria de Escutas Telefônicas. Vol. 1. Coimbra, 2009; by the same author: Das Escutas Telefônicas, Tomo I: A Monitorização dos fluxos informacionais e comunicacionais. Coimbra, 2008. GONZÁLES LÓPEZ, Juan José. Los datos de tráfico de las comunicaciones electrónicas en el proceso penal. Madrid: La Ley, 2007.

possibility of it being apprehended after concretizing the communication, with the transmission of email.

44. Developing informational supports with much greater capacity for memory, at more supportable costs, endorsed the formation, even if temporary, of a database that stores messages sent by email provider services.

45. Consequently, in order to gather proof for criminal processes in the decade of 2000, discussion on the necessity of third-party intervention in email communication became superfluous, because of the supposed risk of losing "*the report*".

46. Central North American legislation (EPCA)[26] and afterwards the effects of the decisions of the European Human Rights Court made themselves felt by internet providers of email services since these ended up with the legal obligation of having to store messages for a determined period of time. The risk of losing the messages, to be used as criminal proof, became significantly reduced.

47. On the other hand, there was growing fear in Europe and in the USA of these new technologies implementing serious crimes, thus stimulating pressure on fundamental rights and invoking, after being repelled in the courts for so long, the idea of balancing risks and benefits as a permissive technique for the quoted interceptions[27].

48. The reaction in favor of fundamental rights to communication (privacy or intimacy, according to any number of arguments) became noteworthy in decisions taken by the European Human Rights Court (EHRC), sentences establishing an understanding on the "*iron cast protection of the right to secrecy of communications, covering not only the content of the communication, but also*

[26] Eletronic Communications Privacy Act (EPCA).
[27] DELMAS-MARTY, Mireille. Por um direito comum. São Paulo: Martins Fontes, 2004, p. 153-162.

encompassing the whole communicative process"[28], with the valorization of the disposition of art. 8 of the European Convention of Human Rights (ECHR)[29].

49. Strengthening tutelage of communications safety is in agreement with the regulation from art. 8 of the ECHR, limiting in a quite rigorous way situations in which such a right may suffer compression within its normative realm.

50. In the first place, according to the ECHR, a reservation of law principle is necessary and in this case the law must be perfectly clear regarding the hypotheses of its incidence and proportional[30] in terms of protected legal goods and the restriction of freedom of communication.

51. The second criteria is submitted to the influence exposed in nº 2, do art. 8 of the ECHR: There may be no interference of public authority in exercising law [regarding private life and communications] except when such interference is guaranteed by law and constitutes a measure that, *in a democratic society*, is necessary to national safety, public safety, the country's economic well-being, maintaining order, and *preventing criminal infractions*, protecting the health or ethics, rights and freedoms of the general population[31].

---

[28] My translation of the text by José Manuel Sánchez Siscart that analyzed a group tried by the European Court of Human Rights (ECHR) on this issue. Medidas de investigación instructoras limitativas de derechos: el secreto de comunicaciones. Política legislativa de la Unión Europea y su repercusión en la legislación y jurisprudencia, **in**: Derecho Penal Europeo. Jurisprudencia del TEDH. Sistemas Penales Europeos. 155. Estudios de Derecho Judicial. Madrid: Consejo General del Poder Judicial, 2010, p. 513.

[29] WINTER, Lorena B. Investigación penal y protección de la privacidad: la jurisprudencia del Tribunal Europeo de Derechos Humanos, **in**: Revista de Proceso, ano 32, nº 152 – out. / 2007, 261-265. SARMIENTO, Daniel, MIERES MIERES, Luis Javier e PRESNO LINERA, Miguel. Las sentencias básicas del Tribunal Europeo de Derechos Humanos: Estudio y jurisprudencia. Navarra: Aranzadí/Civitas, 2007, p. 70. RODRIGUES, Benjamim Silva. Das escutas telefónicas, obra citada, p. 121-7.134-148.

[30] WINTER, Lorena B. Investigación penal y protección de la privacidad: la jurisprudencia del Tribunal Europeo de Derechos Humanos, quoted on p. 167. "*la norma ha de ser suficientemente clara e indicar de manera adecuada a los ciudadanos en qué circunstancias y bajo qué condiciones están las autoridades publicas facultadas para adoptar determinadas medidas que restringen los derechos fundamentales de un ciudadano*".

[31] SÁNCHEZ SISCART, José Manuel, quoted on p. 519.

52. Based on these guidelines, the ECHR reaffirmed the regime of guarantees, conforming to a minimum standard of fundamental rights, even if under pressure of expanding secret criminal investigation measures. Once again, the ECHR deliberated, in the quoted case *Jalloh v. Germany*, on July 11, 2006, that "*even in the most difficult circumstances, such as the struggle against terrorism and organized crime, protecting human rights is not negotiable, beyond any exception or limitation that the Convention itself* [ECHR] *contemplates*"[32].

53. In a scenario of tension between freedom and security and inspired by a rhetoric of risk, States produce norms that, in order to expand resources of criminal repression, end up persecuting human rights.

54. The effects of the ECHR decisions on European criminal legislation were felt in Germany, for example, the law on telecommunications vigilance was submitted to criteria of adequacy extracted from the Federal Constitutional Court agreement on March 3, 2004[33], following the course advocated by the ECHR.

55. Thus what prevails in Europe, just like the North American ECPA from 1986[34][35], is the resolution of only admitting more invasive forms of electronic communications associated to crime prevention (that have still not been committed), with a view towards defending democracy as a whole, consonant with the interpretation of art. 8 of the ECHR. The interpretive stance of the ECHR claims

---

[32] WINTER, Lorena B. Investigación penal y protección de la privacidad: la jurisprudencia del Tribunal Europeo de Derechos Humanos, obra citada, p. 163 (my translation), note 29.

[33] ROGALL, Klaus. A nova regulamentação da vigilância das telecomunicações na Alemanha, quoted on p. 118.

[34] https://www.cdt.org/issue/wiretap-ecpa e http://www.it.ojp.gov/default.aspx?area=privacy&page=1285 , consulted on October 12, 2012.

[35] The EPCA, in harmony with similar European arrangements, restricts access to email, guarantees the respective inviolability of electronic communication, and restricts interventions to serious cases, by court mandate. In order to protect these kinds of measures, always exceptional and conditioned to court mandates issued when there is a probable cause, the legal statute calls for the temporary storage of this information.

www.geraldoprado.com

that intercepting emails must be repudiated as a means of criminal investigation (concerning crimes that have supposedly already been committed)[36].

The (impossible) interception of emails

56. If electronic mail is *"the service that permits exchanging messages among users by means of a network common to all of them"*[37] then the national doctrine must be rigorously interrogated and provoke reflection in the courts on this service as an instrument for private communication.

57. Widening the normative realm of protecting privacy and seeing intimacy as its most restricted circle is befitting of communication, whenever such communication is private.

58. "Communication, differently from information, presupposes an intersubjective relationship whose purpose is transmitting a message"[38]. Private communication should be understood as that which takes place between determined actors, independent from their number. Private communication presupposes that the receptor (or receptors) has been previously determined by that actor emitting the message[39].

59. For reasons exclusive to the actors themselves, in private communication these decide their public, i.e., the actor participating in the communicational process decides the circle of persons that mean intervene

[36] ROGALL, Klaus. A nova regulamentação da vigilância das telecomunicações na Alemanha, quoted on p. 120-121. There are, however, varied forms of electronic surveillance. This presentation is more interested in examining the legal regime and the legislative trend regarding methods of intercepting email, thus restricting the analysis to this hypothesis.
[37] ZANIOLO, Pedro Augusto. Crimes modernos: o impacto da tecnologia no Direito, quoted on, p. 168-9.
[38] CASTANHEIRA NEVES, Rita. As ingerências nas comunicações eletrônicas em processo penal: natureza e respectivo regime jurídico do correio eletrônico enquanto meio de obtenção de prova. Coimbra, 2011, p. 15.
[39] CASTANHEIRA NEVES, Rita. Quoted on, p. 18. LOPES, José Mouraz. Escutas telefônicas: seis teses e uma conclusão, **in**: Revista do Ministério Público, year 26, nº 104 – Oct-Dec 2005. Lisbon, p. 142.

www.geraldoprado.com

therein[40], and, as such, it's up to the State to guarantee the inviolability of private communication (the right to a determined public).

60. Tércio Sampaio Ferraz points out that in Brazil what prevails is tutelage in communications, regarded as an autonomous constitutional legal good, extracted from the normative precept of inc. XII of article 5, whose instrument of protection is confidentiality. In his words:

> *"Confidentiality, in inc. XII of art. 5, refers to* ***communication****, in the interest of defending privacy. This may be seen in the text in two blocks: the Constitution speaks in confidentiality 'of telegraphic correspondence and communications, of telephone data and communications'. Observe how the article may be characterized as a block; the conjunction unites correspondence with telegphaphics, followed by a coma and, afterwards, the conjunction of data is united with telephone communications. There's symmetry between the two blocks. Obviously what's being regulated is* ***communication*** *by way of correspondence and telegraphy and* ***communication*** *of data and telephone equipment. What goes against the incommunicability of confidentiality is interfering in third-party* ***communication,*** *in such a way that what should remain strictly between persons communicating privately is illegally passed on to a third party."* [41]

61. The constitutional legal good, thus, is communication, which guarantees the privacy of the content of a report communicated that forms the message.

62. It's evident that protecting the message communicated against the illegitimate intervention of a third party, whether public or private, takes into consideration the structure of guarantees, in its morphology, and the support used in the message, and also the person responsible for the message.

---

[40] CASTANHEIRA NEVES, Rita. Quoted on, p. 33.

[41] SAMPAIO FERRAZ, Tercio. Parecer **in**: Revista do Instituto dos Advogados de São Paulo, ano 5, nº 9, Jan-June, 2002, p. 162.

63. In the same way that messages make use of physical support, such as traditional correspondence, those responsible for the communication must preserve its confidentiality, leaving the letter untouched. When the communication is made by way of data[42], the responsible agent is equally responsible, since this agent places the data into circulation, and as such must protect the flow of this information by preserving its confidentiality.

64. This doesn't only mean that such confidentiality must only be protected by the State, in the hypotheses the State would bear responsibility by executing/instrumentalizing the communication process, but also the private entity that, in communicating by email, administrates such communication, with a provider for email services from the Internet.

65. As Castanheira Neves emphasizes, private entities must abstain in the same way from any sort of mismanagement of electronic communication[43].

66. In this new scenario the consequence of private services administrating communication channels by which private communication navigates is the obligation of confidentiality, thus being endowed with the right to resist illegitimate intentions to interfere in communication under their responsibility.

67. This leads to the comprehension that the § 160 of German procedural law disciplines the legitimate refusal to hand over evidence handled by media employees, under the protection of the same professional secrecy that

[42] It's worth recalling that Canotilho and Vital Moreira defined data as "*conventional representations of information, under analogical or digital form, which allow for it to be treated automatically*". GOMES CANOTILHO, Joaquim J. and MOREIRA, Vital. Constituição da República Portuguesa Anotada, vol. 1, 4ª ed. Coimbra, 2007, p. 550-1.
[43] CASTANHEIRA NEVES, Rita. Quoted on p. 31.

excludes lawyers and doctors[44]. Article 384 of the Portuguese Criminal Code protects the duty of confidentiality of all those who, by force of their positions or because of them, have had access to private information[45]

68. It seems evident, but it's worth reprising that the duty to collaborate in the hypotheses of obligation of confidentiality does not prevail. This should not be confused with, as Luca Lupária suggests, incriminating employees of internet provider services when these have taken part in criminal complicity with users of such internet services, hypotheses taken up in the cybercrime Convention in the European Council and the Communitarian Guidelines respectively (nº 2000/31, 2002/58 and 2006/24)[46] and that should be interpreted in Brazil within the frame of the aforementioned guarantees.

69. The constitutional statute of inviolability of electronic communications is thus articulated with State obligations regarding criminal repression. If electronic communication is inviolable, demands of adjudicating criminal responsibility legitimatized by a level of truth that makes handing out punishment possible demands that a means be found by which this interest may be harmonized in a constitutionally based way.

70. In this context I understand that the compatibility between the inviolable right to email communication and tutelage of collective interests must

---

[44] ROGALL, Klaus. A nova regulamentação da vigilância das telecomunicações na Alemanha, **in**: 2º Congresso de Investigação Criminal. Coimbra: Almedina, 2010, p. 134-5. Law nº 9.983/00 altered articles 153 and 325 of the Criminal Code that regulate professional secrecy, but didn't discipline in a satisfactory way the problem of confidentiality of email correspondences, nor did it modify article 207 of the Criminal Procedural Code. Even so it is still possible to extract from the Constitution in its article 5, inc. XII, the obligation of confidentiality in order to protect media employees responsible for administrating internet email providers.

[45] FARIA COSTA. José Francisco. A telecomunicações e a privacidade: o olhar (in)discreto de um penalista, **in**: Direito Penal da Comunicação: Alguns escritos. Coimbra, 1998, p. 166.

[46] LUPÁRIA, Luca *et alli*. Internet provider e giustizia penale: modelli di responsabilità e forme de collaborazione processuale, quoted on p. 5.

www.geraldoprado.com

be guaranteed respecting the proportional reservation law - which still doesn't exist - recognizing the apprehension of messages stored in databases.

71. This obviously implies the need of a due legal process which in Brazil, by virtue of the Federal Constitution, is recognized expressively in art. 5, inc. LIV[47].

72. In general terms, a law on seizing emails must contemplate the same aforementioned legal requirements in a generic way as mentioned in items 50 and 51, which are foreseen even though they need greater treatment, in the case of telephone interceptions.

73. Criminal proof produced outside of these parameters is illegal and frustrates the objectives founding the inc. LVI of article 5 of the Federal Constitution of Brazil[48], whose tutelage offers protection of fundamental rights, among which include the inviolability of communication.

Conclusion

74. The positive results in terms of criminal responsibility, which are obtained throughout the world without inappropriately curtailing public liberties, serve to reveal the falsity of the premise used by the authoritarian intellectual Francisco Campos, sometimes unconsciously and uncritically endorsed by part of Brazil's legal doctrine: in a democracy there's no litigation between "individual rights" and "the common good".

[47] In the USA, after a long process that was taken up by Michael J. Philllips, the result of the interpretation/application of the 5th and 14th Amendments of the Constitution. The *Lochner* Court, Myth and Reality: Substantive Due Process from the 1890s to the 1930s. Praeger, 2001. Landmark Supreme Court Cases: The most Influential Decisions of the Supreme Court of the United States. Org. Gary Hartman and others. New York, Facts on File, 2004, p. 151 and the following pages, and Constitutional Law: principles and policies, 4th ed. Erwin Chemerinsky. New York, Wolters Kluwer Law and Business, 2011, p. 511/2.

[48] "LVI – evidence obtained through illicit means are unacceptable in the process;

75. To the contrary, the common good is reaffirmed by scrupulous respect for fundamental rights.

76. The Federal Supreme Court highlights that acting outside of the proper legal parameters in order to obtain proof[49], on the one hand, harms the criminal process, since the proof may be handed over for the judge to evaluate, and on the other, converts a private being contributing towards producing proof into the author of illicit conduct.

77. Three final considerations: a) The 1988 Constitution benefitted from the results of discussion on the Portuguese and Spanish constitutions, States that, just like Brazil, had made the transition from authoritarian to democratic regimes.

78. One of the advantages of Brazil's later entrance into the community of democratic traditions is this country conferring a more rigorous treatment of the problem of illicit proof than that deferred by the Portuguese constitution.

79. In Brazil, illicit proof is not null. Its invalidity is more accentuated. While nullities, even absolute ones, may be convalidated through a general remediating clause, illicit proof is "inadmissible" such as intended by inc. LVI of the aforementioned article 5.

80. Hence the devastating quality to the adequacy of the process, generated by obtaining proof in an illicit fashion, a situation created by obtaining proof by illicit means - violating the correct legal process - must be taken into consideration.

---

[49] Habeas corpus nº 73.338-7. 1st STF group. Narrator: Minister Celso de Mello. Published in notebook nº 1.855-02 of the Federal Supreme Court.

81. b) As regards the relationship between proof and individual rights, the respected professor Leonardo Greco has emphasized that: there are limits to probative activities that must be considered as unsurpassable because of the necessity of protecting the impenetrable core nucleus of personality rights, "to which one must even give up the elevated ideal of discovering the truth"[50].

82. c) Problems associated with email services based abroad have been ignored in this analysis, as guardians of the duty to protect communications privacy.

83. I believe, however, that if once it was possible to recognize the advances of international legal cooperation, which through direct assistance have shortened to path of rogatory letters, both slow and inefficient, now a better way of examining the issue is provided by the project of the new Criminal Procedural Code, which declares in its article 726, that: "Direct assistance will be used when: I – it is provided for in the treaty; II – *it may be submitted to the wide cognition of the competent legal authority*".

84. Thus, by preserving the mechanisms of monitoring the proper legal process, criminal repression confers legitimacy since it is harmonized with the expectations of a State of Law.

Rio de Janeiro, May 31, 2013.

Geraldo Prado

[50] GRECO, Leonardo. Limitações probatórias no processo civil, **in** Temas para uma Perspectiva Crítica do Direito: Homenagem ao Professor Geraldo Prado, 2ª ed. Rio de Janeiro, Lumen Juris, 2012, p. 564.