# RELATÓRIO FINAL
# PIBIC/CNPq/IBMEC-RJ

## 1. IDENTIFICAÇÃO

| |
|---|
| **Nome do(a) bolsista:** Heloisa Alves de Paiva Josephson |
| **Nome do(a) orientador(a):** Profª Ana Maria Esteves de Souza. Doutora em Direito Internacional e da integração Econômica. |
| **Curso:** Direito |
| **Título do Projeto:** Limites e possibilidades jurídicos da vigilância cyber face à soberania dos Estados e ao direito à privacidade. |
| **Três palavras-chave:** vigilância cibernética, direito à privacidade, contra-terrorismo, Edward Snowden |
| **Vigência:** 01.08.2016 – 31.07.2017 |

## 2. INTRODUÇÃO

Após os ataques terroristas de 11 de Setembro de 2001 nos Estados Unidos, realizados pela organização fundamentalista Al Qaeda, o então presidente norte-americano, George W. Bush, instituiu o controverso decreto conhecido como *Patriot Act*[1], com o alardeado objetivo de coibir novas ações terroristas. De forma não militar, o ato governamental exposto autorizava a prática da intercepção em diversos mecanismos de comunicação, relativizando as

[1] Aprovado em 24 de Outubro de 2001- 107º Congresso, 1ª Sessão. Após várias prorrogações durante o governo Bush, em 27 de Julho de 2011, o presidente Barack Obama sancionou a extensão do *USA PATRIOT ACT*, por mais quatro anos - até 2015. Em junho de 2015, várias provisões do *Patriot Act* expiram, sendo substituído pelo *USA Freedom Act*, aprovado pelo congresso americano. Apesar de manter algumas provisões da antiga lei, o *Freedom Act* traz diversas mudanças, dentre elas regras sobre manuseio de dados e quem pode guardar informações obtidas pela NSA. Cf. em: ***"USA Freedom Act: What's in, what's out"***, The Washington Post, publicado em 02 de junho de 2015. Acesso em 09/08/2017 https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

exigências de praxe, dispensando até, em alguns casos, prévia autorização por ordem judicial, como acontecia no caso da vigilância cibernética.[2]

Entretanto, em junho de 2013, Edward Snowden enviou documentos ao jornal *"The Guardian"* informando que a NSA (Agência de Segurança dos Estados Unidos), calcada no "*Patriot Act"* e extrapolando seus limites, realizava uma espionagem em massa em toda sociedade mundial. Os programas utilizados se destinavam à coleta de dados envolvendo chamadas telefônicas, mensagens de textos, vídeos e áudios transmitidos através dos usuários do meio eletrônico, a fim de ampliar a vigilância em massa realizada pelos diversos sistemas de inteligência, bem como foi demonstrado que entidades e agentes públicos de diversos países foram espionados.[3]

Diante desse panorama, por meio do estudo realizado, que estará sintetizado no presente relatório, procurou-se analisar a vigilância cibernética realizada pelos Estados, observando-se os impactos negativos e a repercussão causada no sistema jurídico internacional, a partir da análise dos documentos oficiais da NSA trazidos por Snowden, por meio dos quais foi verificado que as interferências desempenhadas se demonstravam excessivas na vida de milhares de pessoas, inclusive de agentes políticos como Dilma Rousseff e Ângela Merkel e empresas nacionais, como a Petrobrás. [4]

Atualmente, percebe-se que a internet é considerada um local de armazenamento e fornecimento de conhecimento, informação e mídia, sendo essencial para intercomunicação global, bem como observou-se que as inovações tecnológicas aperfeiçoaram as relações humanas. Entretanto, foi constatado que os avanços no meio cibernético facilitaram as interferências governamentais de caráter abusivo realizadas pelos Estados Unidos, que resultavam em uma violação aos direitos humanos. [5]

Dessa forma, asseverou-se que a fundamentação da predominância da garantia da segurança nacional face ao direito à privacidade, diante das interferências no meio digital efetuadas pela NSA, servia apenas como subterfúgio para dar legitimidade à vigilância

---

[2] *Patriot Act* "Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism and Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses."

[3] PEDROSA, Leyberson; MATSUKI, Edgard; **"Entenda o caso Snowden; Petrobras também é alvo de espionagem"**, publicado em 28 de agosto de 2013; Acesso em 20/05/2016 http://www.ebc.com.br/tecnologia/2013/08/web-vigiada-entenda-as-denuncias-de-edward-snowden. Ver também GREENWALD, Glenn; KAZ, Roberto; CASADO, José **"EUA espionaram milhões de e-mails e ligações de brasileiros"**, publicado em 06 de julho de 2013; Acesso em 20/05/2016; http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934.

[4] KHALIL, Chantal; "**Note – Thinking Intelligently About Intelligence: A model Global Framework protecting Privacy** - The George Washington Law Review, volume 47, 2015 – Página 105**"**

[5] PURKAYASTHA, Prabir; BAILEY, Rishab "**U.S. Control of the Internet – Problems facing the Movement to International Governance** - Monthly Review July – August 2014"; 2014; Páginas 104-105".

cibernética excessiva que era executada, quando na verdade esta era usada para uma dominação econômica e política em âmbito mundial e ocasionava violações a direitos humanos protegidos internacionalmente, como o direito à privacidade e liberdade de expressão.

Ademais, também analisou-se que a natureza transnacional da coleta de informações híbridas de agentes públicos e privados atravessa a fronteira dos Estados, dissociando da idéia inicial de garantia da segurança nacional, fazendo com que se produza informação de forma a desprezar a limitação que os direitos dos usuários da internet poderiam causar em seus projetos. Dessa maneira, surge uma discussão quanto à necessidade de regulamentação das atividades realizadas no meio eletrônico, a fim de impedir que violações a esses direitos continuem ocorrendo.[6]

A partir disso, foram consideradas as legislações existentes no que diz respeito à proteção do direito à privacidade e feito um contraponto com a necessidade de garantia da segurança pública, observando-se ainda os entendimentos referentes à sua aplicação no contexto da vigilância cibernética e os impactos negativos causados pela inexistência de uma norma específica que a regulamente.

## 3. JUSTIFICATIVA

A presente pesquisa procura demonstrar a necessidade de um balanceamento entre o direito à privacidade e a garantia à segurança nacional, a fim de averiguar as condições em que um princípio poderia prevalecer frente a outro sem que este sofresse uma restrição abusiva e ilegal por parte de um Estado soberano.

Por meio disto, verificamos através do estudo realizado a inexistência de uma legislação internacional especifica para dispor no que diz respeito às vigilâncias cibernéticas no meio digital, ocasionando uma insegurança jurídica, tendo em vista que passaram a existir interpretações díspares quanto à aplicação das convenções vigentes ao meio eletrônico.

No momento em que analisamos os resultados obtidos na presente pesquisa, perceberemos que é de suma importância a realização de uma discussão quanto à criação de uma legislação internacional própria que possa regulamentar e controlar o uso da vigilância

---

[6] BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WAKER, R.B.J. “**Após Snowden: Repensando o Impacto da Vigilância (After Snowden: Rethinking the impact of Surveillance)** - Revista Eco Pós: Tecnopolíticas e vigilância volume 18; nº 2, 2015, Página 14.”

cibernética pelos Estados, havendo uma disposição inicial sobre o assunto na Resolução 68/167, adotada pela ONU no dia 18 de Dezembro de 2013. [7]

Através da implementação da referida resolução, buscou-se reafirmar a proteção dos direitos humanos contidos nos tratados internacionais vigentes já mencionados, além de requisitar que os Estados revissem seus respectivos procedimentos e disposições legais no que diz respeito à vigilância cibernética, para impedir que essa atuação tivesse um impacto nocivo aos direitos humanos.

De maneira complementar, o Relatório realizado no dia 08 de março de 2016 enfatizou a necessidade de ampliação da proteção ao direito à privacidade dentro do meio digital, criando-se um plano de medidas que continham dez pontos a serem seguidos para adquirir resguardá-lo de maneira efetiva. [8]

Assim, demonstrou-se necessário o debate sobre a necessidade de mudança do tratamento ao direito à privacidade conforme os avanços tecnológicos na era digital, devendo este ser efetivado por mudanças legislativas que cuidem da vigilância cibernética.

## 4. OBJETIVOS

- Observar o contexto envolvendo a vigilância cibernética e seu objetivo;
- Investigar os impactos negativos causados por uma vigilância cyber abusiva;
- Relacionar o direito à privacidade com a necessidade de garantia da segurança pública;
- Avaliar a legislação internacional referente à garantia ao direito à privacidade no meio cibernético;
- Analisar a aplicação e interpretação da legislação internacional existente com relação à proteção do direito à privacidade e a realização da vigilância cibernética;
- Analisar possíveis soluções que minimizariam impactos negativos causados pela vigilância cibernética.

[7] **Resolution adopted by the General Assembly on 18 December 2013**; nº 68/167. The right to privacy in the digital age

[8] **Report of the Office of the United Nations High Commissioner for Human Rights**, implementado no dia 19 de dezembro de 2014.

## 5. REVISÃO DE LITERATURA

Preliminarmente, analisamos a legislação internacional pré-existente em âmbito internacional, a fim de realizar uma investigação da situação jurídica no que diz respeito à vigilância cibernética. Com isso, partimos para o estudo dos tratados internacionais que dispõe quanto à proteção ao direito à privacidade, observando-se que esta é difundida em diversas convenções internacionais.

Assim, verificamos que a proteção à privacidade encontra-se disposta, por exemplo, nos artigos 12 da Declaração Universal de Direitos Humanos[9], no artigo 17 (1) do Pacto Internacional dos Direitos Civis e Políticos[10] e no artigo 11 da Convenção Americana de Direitos Humanos (Pacto San Jose da Costa Rica) [11]. De forma semelhante, a própria Carta das Nações Unidas (Carta da ONU), em seus artigos 2.4 e 2.7[12], defendeu a proibição a qualquer tipo de interferência entre os Estados soberanos, protegendo também o direito à privacidade dos cidadãos.

Durante a continuação do exame dos tratados internacionais, notamos uma relativização do direito à privacidade em casos de ordem pública e interesse público, como, por exemplo, para proteção da segurança nacional. Assim, demonstrou-se que o direito à privacidade não é absoluto, havendo a possibilidade das interferências ocorrerem nos casos

---

[9] **Declaração Universal de Direitos Humanos** " Artigo 12: Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo homem tem direito à proteção da lei contra tais interferências ou ataques" Adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas em 10 de dezembro de 1948

[10] **Pacto Internacional sobre Direitos Civis e Políticos** "Artigo 17: 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas." Incorporado pelo Brasil por meio do Decreto nº 592 de 6 de Julho de 1992.

[11] **Convenção Americana de Direitos Humanos** " Artigo 11: 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2.Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3.Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.", incorporada pelo Brasil por meio do Decreto nº 678 de 06 de novembro de 1992.

[12] **Carta da ONU de 1945** "Artigo 2. A Organização e seus Membros, para a realização dos propósitos mencionados no Artigo 1, agirão de acordo com os seguintes Princípios: (...) 4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas. (...)7. Nenhum dispositivo da presente Carta autorizará as Nações Unidas a intervirem em assuntos que dependam essencialmente da jurisdição de qualquer Estado ou obrigará os Membros a submeterem tais assuntos a uma solução, nos termos da presente Carta; este princípio, porém, não prejudicará a aplicação das medidas coercitivas constantes do Capitulo VII." , incorporada pelo Brasil por meio do Decreto nº 19.841, de 22 de outubro de 1945.

necessários, conforme observado nas disposições dos artigos 51 da Carta da ONU[13] e 27.1[14] da Convenção Americana de Direitos Humanos.

Entretanto, a partir da apreciação das disposições legais acima, pudemos apurar que inexiste qualquer convenção internacional que estabeleça princípios e regule a atividade de vigilância cibernética realizada pelos Estados soberanos. Dessa forma, mesmo que existissem tratados internacionais protegendo o direito à privacidade, havia uma lacuna legal quanto à sua aplicação no meio cibernético, o que gerou interpretações díspares quanto à amplitude das convenções mencionadas.

Com tal característica podemos mencionar que, através de um posicionamento minoritário com relação à aplicabilidade do Pacto Internacional de Direitos Civis e Políticos, os Estados Unidos afastam a proteção ao direito à privacidade consagrada em seu artigo 17, ao afirmar que sua utilização era restrita aqueles indivíduos que estivessem em seu território ou sob sua jurisdição, não aplicando-se em caráter extraterritorial. [15]

Em um sentido neoliberal, também defendido pelos Estados Unidos, o modelo *multi-stakeholder* exige que os governos desempenhem um papel mínimo na governança da internet, e que qualquer papel realizado seja colocado em igualdade com as demais partes interessadas, além de que qualquer decisão referente à governança da internet seja adquirida por um consenso. Entretanto, tal sistema desconsidera a possibilidade dos Estados que possuem diferentes interesses, bem como as suas respectivas diferenças que impedem que eles estejam em igualdade.[16]

Logo, na ausência de precedentes históricos ou normas que se referem ao espaço cibernético, os agentes de governo criam suas próprias leis para regulamentá-lo[17], conforme

---

[13] **Carta da ONU de 1945** "Artigo 51: Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais" incorporada pelo Brasil por meio do Decreto nº 19.841, de 22 de outubro de 1945.

[14] **Convenção Americana de Direitos Humanos** " Artigo 27.1: Em caso de guerra, de perigo público, ou de outra emergência que ameace a independência ou segurança do Estado Parte, este poderá adotar disposições que, na medida e pelo tempo estritamente limitados às exigências da situação, suspendam as obrigações contraídas em virtude desta Convenção, desde que tais disposições não sejam incompatíveis com as demais obrigações que lhe impõe o Direito Internacional e não encerrem discriminação alguma fundada em motivos de raça, cor, sexo, idioma, religião ou origem social" incorporada pelo Brasil por meio do Decreto nº 678 de 06 de novembro de 1992.

[15] SINHA, G. Alex; "**NSA Surveillance since 9/11 and the human right to privacy** - Loyola Law Review, 2014; volume 59; Página 902."

[16] PURKAYASTHA, Prabir; BAILEY, Rishab. "**U.S. Control of the Internet – Problems facing the Movement to International Governance -** Monthly Review July – August 2014; 2014; Páginas 112-117."

[17] KANUCK, Sean; "**Sovereign Discourse on Cyber Conflict Under Internacional Law** - Texas Law Review; vol. 88; 2010; Página 1585".

podemos averiguar na criação do Marco Civil da Internet, que seria uma criação legislativa brasileira que busca proteger os direitos humanos dos usuários do meio cibernético e o próprio *Patriot Act*, que foi criado para autorizar as interceptações realizadas a fim de prevenir ataques terroristas futuros.

Da mesma forma, houve uma tentativa de adaptação legislativa para responsabilização dos Estados, a fim de aplicar as leis de conflitos armados para os ataques cibernéticos, denominado *"Tallinn Manual on the International Law Applicable to Cyber Warfare"* ou também conhecido como *"Manual"*. Por meio dele, averiguou-se que promover um grupo de *malware* constitui o uso da força e violaria o artigo 2(4) da Carta da ONU. [18]

Todavia, o Manual indica que uma simples ajuda financeira ou fornecimento de refúgio para grupos que realizam o ataque cibernético não constituiria o uso da força, impedindo a responsabilização dos Estados. A partir de uma maior analise dele, percebemos que ele é pouco claro quanto à internacionalização dos conflitos e a respectiva responsabilização dos Estados. [19]

Além disso, uma decisão advinda do Caso Lotus, na Corte Permanente de Justiça Internacional, por meio da qual foi decidido que, na ausência de uma norma positivada, o Estado teria liberdade para atuar como desejasse, isto é, ele possuiria uma margem de decisão em adotar os princípios que julgar mais adequados ao caso concreto, sendo apenas limitado nos casos em que há normas proibitivas. Desse modo, muitos governos defendem esta abordagem como a melhor forma de compreender a espionagem no âmbito legislativo internacional e, portanto, por inexistir legislação internacional que a proíba ou regule, os Estados estão livres para realizar a vigilância cibernética que desejarem. [20]

Por outro lado, há quem afirme que a legislação internacional proíbe a espionagem, justificando através do princípio da soberania, em que um Estado não poderia interferir no âmbito interno de outros, bem como mencionam que a proteção conferida pelo artigo 17 do Pacto Internacional de Direitos Civis e Políticos deveria ser ampliado para interferências e coleta de dados realizados no meio eletrônico. [21]

Pelo exposto, percebeu-se que a falta de um dispositivo legal próprio para a vigilância cibernética gera uma insegurança jurídica em âmbito internacional, tendo em vista

---

[18] MARGULIES, Peter; "**Sovereignty and Cyber Attacks: Technology´s Challenge to the Law of State Responsibility**; Melbourne Jornal of International Law; volume 14; 2013, páginas 497-498.
[19] *Ibidem*, Páginas 510-511.
[20] DEEKS, Ashley; "**An international Legal Framework for surveillance** - "Virginia Journal of International Law; 2015, volume 55:2, páginas 301-302"
[21] *Ibidem*, páginas 306-313.

as diversas interpretações que são geradas quanto à aplicação ou não dos tratados internacionais no meio digital.

## 6. METODOLOGIA UTILIZADA

Inicialmente, foi realizado um levantamento bibliográfico do tema. A partir dele, utilizamos diversos artigos científicos e também uma notícia jornalística que abordaram o tema do presente estudo exposto. Ademais, foram analisadas legislações, resoluções e decisões internacionais no que diz respeito ao direito à privacidade.

Por fim, a partir da junção das informações analisadas, realizamos uma crítica quanto à situação jurídica existente no âmbito internacional, bem como expusemos tentativas de adaptação legislativa quanto ao tema e a necessidade de criação de uma legislação clara para buscar a criação de limites e sanções na utilização do meio digital para fins de vigilância.

## 7. ANÁLISE DOS RESULTADOS ALCANÇADOS

Com os estudos efetuados em função da pesquisa em tese, compreendeu-se a importância da vigilância para a atividade estatal, objetivando conter possíveis ataques terroristas e garantir a segurança nacional. Entretanto, ao mesmo tempo, pôde-se perceber que a vigilância pode, por vezes, se configurar como excessiva, de modo a violar direitos humanos protegidos por tratados internacionais vigentes, como direito à privacidade e liberdade de expressão.

Para impedir entendimentos díspares causados pela falta de legislação internacional específica no que tange a vigilância cibernética, torna-se necessária a criação de uma convenção internacional eficaz e específica quanto à proteção dos direitos humanos no meio digital, a fim de atenuar os impactos negativos resultantes de uma possível vigilância excessiva, tendo em vista que a falta de uma legislação internacional específica quanto às vigilâncias cibernéticas, causa uma insegurança jurídica no meio internacional, já que os Estados realizariam suas interceptações sem qualquer tipo de controle ou limitação.

A criação de uma legislação internacional serviria como uma ampliação à proteção dos direitos fundamentais já defendidos em diversas convenções internacionais já elucidadas e serve como uma garantia de diminuição nos casos de vigilância excessiva no âmbito digital, já que preenche uma lacuna na legislação internacional e impede

interpretações prejudiciais à população mundial quanto à proteção do direito à privacidade e a aplicação dos tratados já existentes. .

Por meio do exposto, percebeu-se que internet sem qualquer tipo de controle é inviável, sendo necessária a criação de mecanismos que garantam liberdade aos usuários no meio cibernético e a possibilidade de entidades estatais a utilizarem como forma de garantia da segurança nacional. Entretanto, da mesma forma, também é necessário que haja uma regulamentação que impeça qualquer abuso nas atividades desenvolvidas no meio eletrônico que possam violar direitos humanos dos próprios usuários e, caso estas ocorram, é também imprescindível constituição de remédios para solucionar os danos causados.

A partir da análise de artigos científicos e notícias jornalísticas existentes com relação ao direito à privacidade no meio digital, bem como da legislação internacional vigente e das tentativas de adaptação legal para aplicar tal direito no meio digital, obtivemos uma maior compreensão do direito à privacidade em âmbito internacional e realizamos o artigo em anexo.

O referido artigo foi criado delineando o conflito entre o direito à privacidade, a soberania dos Estados, direito à segurança e interesse público, expondo a necessidade de criação de uma legislação internacional clara e eficaz no que diz respeito à aplicação do direito à privacidade nas atividades de vigilância cibernética realizada pelos Estados, impedindo que haja as interpretações díspares quanto à aplicação ou não de tratados internacionais nesses casos.

Dado o prazo do presente projeto (PIBIC), inicialmente previsto para ser executado em 12 meses, ter sido reduzido para 6 meses, não houve ainda tempo hábil para submeter o artigo a eventos acadêmicos – o que, todavia, ainda será realizado.

## 8. REFERÊNCIAS


1. BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WAKER, R.B.J. **“Após Snowden: Repensando o Impacto da Vigilância (After Snowden: Rethinking the impact of Surveillance)** - Revista Eco Pós: Tecnopolíticas e vigilância volume 18; nº 2, 2015 – páginas 8-35.”
2. CANNATACI, Joseph A. **Report of the Special Rapporteur on the right to privacy.**
3. **Carta da ONU de 1945**, incorporada pelo Brasil por meio do Decreto nº 19.841, de 22 de outubro de 1945.

4. **Convenção Americana de Direitos Humanos** Assinada na Conferência Especializada Interamericana sobre Direitos Humanos,San José, Costa Rica, em 22 de novembro de 1969.

5. **Declaração Universal de Direitos Humanos** - Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948.

6. DEEKS, Ashley; "**An international Legal Framework for surveillance** - "Virginia Journal of International Law; 2015, volume 55:2, páginas 291-368"

7. GREENWALD, Glenn; KAZ, Roberto; CASADO, José "**EUA espionaram milhões de e-mails e ligações de brasileiros**", publicado em 06 de julho de 2013; Acesso em 20/05/2016; http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934.

8. KANUCK, Sean; "**Sovereign Discourse on Cyber Conflict Under Internacional Law** - Texas Law Review; vol. 88; 2010; páginas 1571-1597."

9. KHALIL, Chantal; "**Note – Thinking Intelligently About Intelligence: A model Global Framework protecting Privacy** - The George Washington Law Review, volume 47, 2015 – páginas 919-947"

10. **Marco Civil da Internet**, Lei nº 12.965, promulgada dia 23 de Abril de 2014.

11. MARGULIES, Peter; "**Sovereignty and Cyber Attacks: Technology´s Challenge to the Law of State Responsibility**. Melbourne Jornal of International Law; volume 14; 2013, páginas 496-519"

12. MATTOS, Sayonara Gonçalves da Silva; **"A importância da proporcionalidade e da ponderação de interesses na solução do conflito entre os princípios jurídicos**, publicado na edição 16, do dia 23 de fevereiro de 2007 na Revista da Doutrina TRF4."

13. MILANOVIC, Marko "**Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age** - Harvard International Law journal / Vol 56;number 1, winter 2015"; 2015; páginas 81-146".

14. **Pacto Internacional de Direitos Civis e Políticos** - Incorporado pelo Brasil por meio do Decreto nº 592 de 6 de Julho de 1992.

15. **Patriot Act** - Promulgado em 24 de Outubro de 2001- 107º Congresso, 1ª Sessão.

16. PEDROSA, Leyberson; MATSUKI, Edgard; "**Entenda o caso Snowden; Petrobras também é alvo de espionagem**", publicado em 28 de agosto de 2013; Acesso em 20/05/2016 http://www.ebc.com.br/tecnologia/2013/08/web-vigiada-entenda-as-denuncias-de-edward-snowden.

17. PILATI, José Isaac; OLIVO, Mikhail Vieira De "**Um novo olhar sobre o Direito à Privacidade: caso Snowden e pós modernidade jurídica (A new look at the right to privacy: Case Snowden and legal postmodernity)** - V Seminário Diálogo Ambiental, Constitucional e Internacional, Sequência (Florianópolis), nº 69, 2014 – páginas 281-300."

18. PURKAYASTHA, Prabir; BAILEY, Rishab "**U.S. Control of the Internet – Problems facing the Movement to International Governance** - Monthly Review July – August 2014"; 2014; Páginas 103-125".

19. **Report of the Office of the United Nations High Commissioner for Human Rights**- General Assembly - Human Rights Council

20. Resolution adopted by the General Assembly on 18 December 2013; nº 68/167. **The right to privacy in the digital age**;

21. SINHA, G. Alex; “**NSA Surveillance since 9/11 and the human right to privacy** - Loyola Law Review, 2014; volume 59; páginas 861-946”

22. **“USA Freedom Act: What’s in, what’s out**”, The Washington Post, publicado em 02 de junho de 2015. Acesso em 09/08/2017 https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

“

**LOCAL: Rio de Janeiro**

**DATA: 15 de Agosto de 2017**

**ASSINATURA DO(A) BOLSISTA:**

**ASSINATURA DO(A) PROFESSOR(A) ORIENTADOR(A):**

**ASSINATURA DO(A) ORIENTADOR(A):**