Data Protection in the USA

The revolutionary technologies, such as Internet and Data Science, created the necessity of treat with strict legality the personal data of humans beings, going further in the discussion of rights like privacy.

As in every Jurisdiction, the basic rule is that there is no privacy for citizens when the national security is in game. But for many other situations, privacy still important, such as in commercial competition, for the protection of consumers or the protection of the intimate of a person.

Also as in many jurisdictions, the normative framework on the data of citizens in the United States got first these four strategic sectors of the society:

(i) the **public security** sector received the *(a)* Controlling the Assault of Non-Solicited Pornography and Marketing Act (18, U.S.C., §1037), the *(b)* Electronic Communications Privacy Act (18, U.S.C., §2510),

Proteção de Dados nos EUA

As tecnologias revolucionárias, como a Internet e a Ciência de Dados, criaram a necessidade de tratar com estrita legalidade os dados pessoais dos seres humanos, indo mais longe na discussão de direitos como a privacidade.

Como em toda Jurisdição, a regra básica é que não há privacidade para os cidadãos quando a segurança nacional está em jogo. Mas para muitas outras situações, a privacidade ainda é importante, como na competição comercial, para a proteção dos consumidores ou na proteção da intimidade de uma pessoa.

Como ocorre em muitas jurisdições, a estrutura normativa sobre os dados dos cidadãos nos Estados Unidos alcançou primeiro esses quatro setores estratégicos da sociedade:

(i) o setor de **segurança pública** recebeu o *(a)* Ato Legislativo sobre o Controle Infracional por Envio de Pornografia e Marketing não solicitados (C.E.U., 18, §1037), o *(b)* Ato sobre Privacidade de Comunicações Eletrônicas (C.E.U., 18, §2510), bem

as well as the *(c)* Computer Fraud and Abuse Act (18, U.S.C., §1030);	como a *(c)* Lei sobre Fraude e Abuso de Computadores (C.E.U., 18, §1030);
(ii) the **health** sector received the *(d)* Health Insurance Portability and Accountability Act (42, U.S.C., §1301 et seq.), as well as the *(e)* Security Breach Notification Rule (45, C.F.R., Part 164);	(ii) o setor de **saúde** recebeu a *(d)* Lei federal de Portabilidade e Responsabilidade de Seguro Saúde (C.E.U., 42, §1301 e seguintes), bem como *(e)* a Regra de Notificação de Violação de Segurança (C.R.F., 45, Parte 164);
(iii) the **commercial** sector received the *(f)* Federal Trade Comission Act (15, U.S.C., §§41-58), as well as the *(g)* Children's Online Privacy Protection Act (15, U.S.C., §§6501-6506) and the *(h)* Controlling the Assault of Non-Solicited Pornography and Marketing Act (15, U.S.C., §§7701-7713);	(iii) o setor **comercial** recebeu a *(f)* Lei da Comissão Federal de Comércio (C.E.U., 15, §§41-58), bem como a *(g)* Lei de Proteção à Privacidade Online das Crianças (C.E.U., 15, §§6501-6506) e *(h)* Ato Legislativo sobre o Controle Infracional por Envio de Pornografia e Marketing não solicitados (C.E.U., 18, §§7701-7713);
(iv) and the **financial** sector received the *(i)* Financial Services Modernization Act, also called Gramm-Leach-Bliley Act (15, U.S.C., §§6801-6827), as well as the *(j)* Fair Credit	(iv) e o setor **financeiro** recebeu a *(i)* Lei federal de Modernização dos Serviços Financeiros, também chamada Lei Gramm-Leach-Bliley (C.E.U., 15, §§6801-6827), bem como a *(j)* Lei

Reporting Act (15 USC §1681).	de Declaração de Crédito Justo (C.E.U., 15, § 1681).
The Chapters 15 (Commerce and Trade), 18 (Crimes and Criminal Procedure) and 42 (The Public Health and Welfare) of the United States Code (U.S.C.), as well as the Code of Federal Regulations (C.F.R.), Titles 16 (Commercial Practices) and 45 (Public Welfare), constitute the federal normative *locus* of data protection in the USA.	Os Capítulos 15 (Comércio), 18 (Crimes e Processo Criminal) e 42 (Saúde Pública e Bem-Estar), do Código dos Estados Unidos (C.E.U.), bem como o Código de Regulamentos Federais (C.R.F.), Títulos 16 (Práticas Comerciais) e 45 (Bem-Estar Público), constituem o *locus* normativo federal da proteção de dados nos EUA.
Let's understand a little more on each Act in relation with data protection:	Vamos entender um pouco mais sobre cada norma em relação à proteção de dados:
public security:	*segurança pública*:
(a) in the criminal sector, there is the fraud and related activity in connection with eletronic mail and the hacking with spam activity. The federal criminal norm establishes that commit a crime, that generate fine and/or imprisonment for not more than 5 years, "*whoever, in or affecting interstate or foreign commerce,*	*(a)* no setor criminal, há a fraude, bem como a atividade relacionada com esta, em conexão com o correio eletrônico e a atividade de hacking com spam. A norma criminal federal estabelece que comete crime, que gera multa e/ou prisão por não mais de 5 anos, "*quem afetar o comércio, interestadual ou estrangeiro,*

	knowingly—(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer, (2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,..." [18, U.S.C., §1037 (a) (1) (2)] – year 2003	*consciente que—(1) acessa um computador protegido sem autorização, e intencionamente inicia a transmissão de múltiplas mensagens de email comerciais a partir, ou através, de tal computador, (2) usa um computador protegido para transmitir ou retransmitir várias mensagens de correio eletrônico comerciais, com a intenção de enganar ou induzir em erro destinatários, ou qualquer serviço de acesso à Internet, quanto à origem de tais mensagens,...*" [C.E.U., 18, §1037 (a) (1) (2)] – ano de 2003
	(b) concerning <u>communications interception</u>, it is important underline the following norm: "*any person who intentionally—(a) sends through the*	*(b)* em relação à <u>interceptação de comunicações</u>, é importante sublinhar a seguinte norma: "*qualquer pessoa que intencionalmente:*

mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications..." shall be fined and/or imprisoned not more than 5 years [18, U.S.C., §2515 (1) (a)]; being very enlightening this Congressional Finding: "*To <u>safeguard the privacy of innocent persons</u>, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent*	*(a) envie pelo correio, ou envie ou transporte em comércio interestadual ou estrangeiro, qualquer dispositivo eletrônico, mecânico ou outro, conhecendo ou tendo motivos para saber que o design desse dispositivo o torna útil principalmente para fins de interceptação sub-reptícia de comunicações por fio, orais ou eletrônicas...* "será multado e/ou preso por não mais que 5 anos [C.E.U., 18, §2515 (1) (a)]; sendo muito esclarecedora esta constatação do Congresso: "*Para <u>salvaguardar a privacidade de pessoas inocentes</u>, a interceptação de comunicações orais ou cabeadas, em que nenhuma das partes da comunicação consentiu na interceptação deve*

	jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused" (18, U.S.C., §2510) – year 1986;	*ser permitida somente quando autorizada pela Justiça competente e deve permanecer sob o controle e supervisão do tribunal que concedeu a autorização. A interceptação de comunicações por fio e orais deve ser limitada a certos tipos principais de delitos e categorias específicas de crimes com garantias de que a interceptação é justificada e que as informações obtidas por meio delas não serão mal utilizadas* "(C.E.U., 18, §2510) – ano de 1986;
	(c) the Computer Fraud and Abuse Act establishes that a person "*with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication*	*(c)* a Lei de Fraude e Abuso de Computadores estabelece que uma pessoa "*com intenção de extorquir de alguém dinheiro ou outra coisa de valor, transmite em comércio interestadual ou*

containing any—(A) threat to cause damage to a protected computer; (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion; shall be punished" [18, U.S.C., §1030 7 (a) (b) (c)] – year 1986;	*estrangeiro comunicação que contenha—(A) uma ameaça que possa causar danos a um computador protegido; (B) uma ameaça capaz de obter informações de um computador protegido, seja sem autorização, ou em excesso de autorização, ou em exposição de informação confidencial, obtida, de um computador protegido, sem autorização ou por excesso na autorização de acesso"; ou (C) demanda ou solicitação de dinheiro, ou outra coisa de valor, em relação a danos a um computador protegido, onde tal dano foi causado para facilitar a extorsão; será punido"* [C.E.U., 18, §1030 7 (a) (b) (c)] - ano de 1986;
health:	*saúde:*

	(d) concerning health information, the federal norm defines the term '<u>individually identifiable health information</u>' as "*any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the*
	(d) em relação à informação de saúde, a norma federal define o termo '<u>informação de saúde identificável individualmente</u>' como "qualquer informação, incluindo informação demográfica recolhida de um indivíduo, que—(A) é criada ou recebida por um prestador de cuidados de saúde, plano de saúde, empregador, ou câmara de standardização e compensação de serviços de saúde; e (B) se relaciona com a saúde ou condição física ou mental passada, presente ou futura de um indivíduo, a prestação de cuidados de saúde a um indivíduo ou o pagamento passado, presente ou futuro por prestação de serviços de saúde a um indivíduo, e—(i) identifica o

individual" [42, U.S.C., §1320d (6)]; and, for safeguards, the norm establishes that "*Each person ... who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards —(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated— (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person*" [42, U.S.C., §1320d-2 (d) (2)] – year 1996;	*indivíduo; ou (ii) em relação à qual haja uma base razoável para acreditar que a informação pode ser usada para identificar o indivíduo*" [C.E.U., 42, §1320d (6)]; e, como garantias, a norma estabelece que "*cada pessoa ... que mantém ou transmite informações de saúde deve manter salvaguardas administrativas, técnicas e físicas razoáveis e apropriadas— (A) para assegurar a integridade e a confidencialidade das informações; (B) para proteger contra aquilo que pode ser razoavelmente antecipado, como— (i) ameaças ou riscos à segurança ou integridade das informações; e (ii) usos ou divulgações não autorizados da informação; e (C) para assegurar o cumprimento desta parte pelos oficiais*

	e empregados dessa pessoa" [C.E.U., 42, §1320d-2 (d) (2)] – ano de 1996;
(e) the normative regulation give to us important concepts: "*Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes*"; "*Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner*"; "*Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system*" (45, C.F.R., §164.304) – year 2000;	*(e)* o regulamento normativo nos dá conceitos importantes: "*Confidencialidade significa a propriedade de que os dados ou informações não são disponibilizados ou divulgados a pessoas ou processos não autorizados*"; "*Integridade significa a propriedade de que os dados ou informações não foram alterados ou destruídos de maneira não autorizada*"; "*Incidente de segurança significa a tentativa ou sucesso no acesso não autorizado, uso, divulgação, modificação ou destruição de informações ou interferência nas operações do*

	sistema em um sistema de informação" (C.E.U., 45, §164.304) – ano de 2000;
trade and commerce:	*comércio*:
(f) concerning private areas in websites, the Federal Trade Comission Act express that: "*it shall be unlawful for any person—(A) to circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service that is used by the ticket issuer to enforce posted event ticket purchasing limits*" [15, U.S.C., §45c (a) (1)] – years 1914, 2016;	*(f)* em relação a áreas privadas em sites, a Lei da Comissão Federal de Comércio declara que: "*será ilegal para qualquer pessoa—(A) contornar uma medida de segurança, sistema de controle de acesso ou outro controle ou medida tecnológica em um site ou serviço online que é usado pelo emissor do bilhete para impor limites de compra de ingressos para eventos*" [C.E.U., 15, §45c (a) (1)] - anos de 1914, 2016;
(g) in the normative concerning the protection of children using the Internet, it is possible underline	*(g)* na normativa relativa à proteção de crianças que utilizam a Internet, é possível sublinhar essas duas

these two important definitions to data protection: the terms Personal Information and Consent. According the norm, "*the term '<u>personal information</u>' means individually identifiable information about an individual collected online, including—(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number (...)*" [15, U.S.C., §6501 (8)]; and "*the term '<u>verifiable parental consent</u>' means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the*	importantes definições para a proteção de dados: os termos Informações Pessoais e Consentimento. De acordo com a norma, "*o termo '<u>informação pessoal</u>' significa informação individualmente identificável sobre um indivíduo, coletada on-line, incluindo—(A) um primeiro e último nome; (B) um endereço residencial ou outro endereço físico, incluindo nome da rua e nome de um município ou vila; (C) um endereço de e-mail; (D) um número de telefone; (E) um número da Previdência Social (...) "* [C.E.U., 15, §6501 (8)]; e "*o termo '<u>consentimento verificável dos pais</u>' significa qualquer esforço razoável (levando em consideração a tecnologia disponível),*

	notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child" – year 1998;	*incluindo uma solicitação de autorização para futura coleta, uso e divulgação descrita na notificação, para assegurar que os pais de uma criança recebam aviso das práticas de coleta, uso e divulgação de informações pessoais do operador, e autorizem a coleta, uso e divulgação, conforme aplicável, de informações pessoais e o uso subseqüente dessas informações antes que essas informações sejam coletadas da criança"* – ano de 1998";
	(h) concerning non-solicited marketing, the federal norm give to us a clear concept on affirmative consent: "the term '*affirmative consent', when used with respect to a commercial electronic mail*	*(h)* em relação ao marketing não solicitado, a norma federal nos fornece um conceito claro sobre o consentimento explícito/afirmativo: *"o termo 'consentimento afirmativo', quando usado com relação*

message, means that— (A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages" (15, U.S.C., §7702) – year 2003;	*a uma mensagem eletrônica comercial, significa que— (A) o destinatário expressamente consentiu em receber a mensagem, seja em resposta a um pedido claro e expresso para tal consentimento ou por iniciativa própria do destinatário; e (B) se a mensagem for de uma parte que não a parte à qual o destinatário comunicou tal consentimento, o destinatário recebeu um aviso claro e expresso no momento em que o consentimento foi comunicado de que o endereço de correio eletrônico do destinatário poderia ser transferido para a outra parte para esse fim de iniciar mensagens de correio eletrônico comercial*" (C.E.U., 15, §7702) – ano de 2003;

finances:	*finanças:*
(i) the U.S.C., Chapter 15 (Commercial Trade), Chapter 94 (Privacy, §§ 6801-6827), establishes that "*It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information*" (15, U.S.C., §6801) – year 1999;	*(i)* o C.E.U., Capítulo 15 (Comércio Comercial), SubCapítulo 94 (Privacidade, §§ 6801-6827), estabelece que "É política do Congresso que cada instituição financeira tenha uma obrigação afirmativa e contínua de respeitar a privacidade de seus clientes e de proteger a segurança e a confidencialidade das informações pessoais não públicas desses clientes"(C.E.U., 15, §6801) - ano de 1999;
(j) the mechanisms to check the general reputation of consumers of financial products and services, important to maintain fair and	*(j)* os mecanismos para verificar a reputação dos consumidores de produtos e serviços financeiros, importantes para manter relatórios de

accurate credit reporting and credibility to the financial system, need also “*respect for the consumer's right to privacy*” [15, U.S.C., §1681 (a) (4)] – in this meaning, consumer reporting agencies shall adopt *“reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information*” [15, U.S.C., §1681 (b)] – years 1970, 2003.	crédito justos e precisos e credibilidade para o sistema financeiro, também precisam "*respeitar o direito do consumidor à privacidade*" [C.E.U., 15, §1681 (a) (4)] - neste sentido, as agências de informação ao consumidor devem adotar *“procedimentos razoáveis para atender às necessidades do comércio de crédito ao consumidor, pessoal, seguro e outras informações de maneira justa e eqüitativa para o consumidor, no que diz respeito à confidencialidade, precisão, relevância e utilização apropriada de tais informações*” [C.E.U., 15, §1681 (b)] - anos de 1970 e de 2003.
As we can see, the federal norms of USA already provide a high degree of data protection, mainly in the strategic sectors of the society, like public security, health, trade and	Como podemos ver, as normas federais dos EUA já fornecem um alto grau de proteção de dados, principalmente nos setores estratégicos da sociedade, como segurança pública,

finances. Already exist key concepts and mechanisms to avoid, or, at least, mitigate events concerning data breach, spam, unauthorized use of systems. Confidentiality, integrity, cryptography, personal information and consent are terms already presents in the US legal framework.

Let's come back to the year of 1791, with the Amendment IV, to the Constitution of the United States. This basic norm estates that: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*".

But this is enough to protect citizens?

Well, the norm above is the norm that, today, impact the FBI activities concerning the accessing to cell phone location data without a warrant. When public security is in game, the privacy of citizens can be relativized in any way? Or it is necessary observes the legal structure among the Powers?

The US Supreme Court, in the

saúde, comércio e finanças. Já existem conceitos-chave e mecanismos para evitar, ou, pelo menos, mitigar eventos relativos à violação de dados, spam, uso não autorizado de sistemas. Confidencialidade, integridade, criptografia, informações pessoais e consentimento são termos já presentes na legislação dos EUA.

Voltemos ao ano de 1.791, com a Quarta Emenda, da Constituição dos Estados Unidos. Esta norma básica diz que: "*O direito do povo de estar seguro em suas pessoas, casas, documentos e efeitos, contra buscas e apreensões irracionais, não deve ser violado, e nenhuma ordem judicial será emitida, a não ser por uma causa provável, apoiada por Juramento ou afirmação, e particularmente descrevendo o lugar a ser revistado e as pessoas ou coisas a serem apreendidas*".

Mas isto é suficiente para proteger os cidadãos?

A norma acima é a norma que, hoje, impacta as atividades do FBI com relação ao acesso aos dados de localização de celulares sem um mandado. Quando a segurança pública está em jogo, a privacidade dos cidadãos pode ser relativizada de alguma forma? Ou é necessário observar a estrutura legal entre os Poderes?

A Suprema Corte dos EUA, no

case Carpenter v. United States, expressed: "*The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation'" 18 U. S. C. §2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under §2703(d) is not a permissible mechanism for accessing historical cell-site records*" (US Supreme Court, Carpenter v. United States).

Other important case, concerning public security and business cloud storage, is the case United States v. Microsoft Corp, in which the main issue is about the possibility of US Government, aiming to solve a crime, get access to data, that is stored in other jurisdiction by a company with headquarter in USA. On jurisdiction issues, was enacted, at 2018, the Clarifying Lawful Overseas Use of Data Act, or CLOUD Act (18, U.S.C., § 2523).

Well, *juris dictio* (Jurisdiction) has the meaning of connect the sovereign power to a territory, be this a

caso Carpenter vs. Estados Unidos, expressou: "*O Governo não obteve um mandado apoiado por causa provável antes de adquirir os registros do celular de Carpenter. Adquiriu esses registros de acordo com uma ordem judicial apoiada na Lei de Armazenamento de Comunicações, que exigia que o Governo mostrasse 'motivos razoáveis' para acreditar que os registros eram 'relevantes e com materialidade para uma investigação em andamento'" C.E.U., 18, §2703 (d). Essa exibição fica bem aquém da causa provável exigida para um mandado. Consequentemente, uma ordem emitida de acordo com o §2703 (d) não é um mecanismo permissível para acessar registros históricos de torres de celular*"(Suprema Corte dos EUA, Carpenter vs. Estados Unidos).

Outro caso importante, relativo a segurança pública e armazenamento em nuvem comercial, é o caso dos Estados Unidos versus Microsoft, em que a questão principal é sobre a possibilidade do governo dos EUA, visando resolver um crime, obter acesso a dados, os quais são armazenados em outra jurisdição por uma empresa com sede nos EUA. Em questões de jurisdição, foi promulgada, em 2018, a Lei de Esclarecimento sobre Uso de Dados no Exterior, ou Lei da Nuvem (C.E.U., 18, §2523).

Juris dictio (Jurisdição) tem o significado de conectar o poder soberano a um território, seja este um

natural place or a virtual one (.com, .uk, .br, etc). This is always the basic point to structure an efficient legal system. And when we talk about data protection this still being debating in the juridical world of the US.

So, there is a lot to do in terms of data protection, and, maybe, put all these norms together in one big one federal norm, like European Union did, can be a good way to have a whole and deep overview on the data protection issues.

_____

August, 07th 2018

Rafael De Conti
Brazilian Lawyer, as free researcher* of International Law.

* this is not, and can not be, a legal opinion; the only purpose of this text is the comparative studies on data protection laws around the World. For legal opinions and advice on US Law an US Lawyer shall be consulted.

Looking for connected lawyers around the World? check globobroking.com

lugar natural ou um virtual (.com, .uk, .br, etc). Este é sempre o ponto básico para estruturar um sistema legal eficiente. E quando falamos em proteção de dados isso ainda está sendo debatido no mundo jurídico dos EUA.

Portanto, há muito a se fazer em termos de proteção de dados e, talvez, colocar todas essas normas juntas em uma grande norma federal, como a União Europeia fez, pode ser um bom modo de ter uma visão do todo e profunda sobre as questões de proteção de dados.

_____

7 de agosto de 2018

Rafael De Conti
Advogado brasileiro, na qualidade de pesquisador livre* do Direito Internacional.

* isto não é, e não pode ser, uma opinião legal; o único propósito deste texto é o estudo comparativo das leis de proteção de dados em todo o Mundo. Para pareceres jurídicos e aconselhamento sobre a lei dos EUA, um advogado dos EUA deve ser consultado.

Procurando por advogados conectados ao redor do mundo? verifique globobroking.com

#USDataProtection #CyberLaw #ICTLaw #ITLaw #InternetLaw #TechLaw #DigitalLaw	**#ProtecaoDeDadosEUA** #DireitoCybernetico #DireitoDaTIC #DireitoDaTI #DireitoDaInternet #DireitoDaTecnologia #DireitoDigital
Key-words: Data Protection in the USA, cyber public security, data protection, eletronic mail, hacking with spam activity, communications interception, safeguard the privacy of innocent persons, damage to a protected computer, individually identifiable health information, integrity and confidentiality, unauthorized uses or disclosures, Security incident, circumvent a security measure, access control system, personal information, verifiable parental consent, affirmative consent, privacy, protect the security and confidentiality, consumer's right to privacy, confidentiality, accuracy, relevancy, and proper utilization.	**Palavras-chave**: Proteção de dados nos EUA, segurança pública virtual, proteção de dados, correio eletrônico, atividade de hacking com spam, interceptação de comunicações, grampo, salvaguardar a privacidade de pessoas inocentes, ameaça que possa causar danos a um computador, informação de saúde identificável individualmente, integridade e confidencialidade, usos ou divulgações não autorizados, Confidencialidade, Incidente de segurança, contornar uma medida de segurança, sistema de controle de acesso, informação pessoal, consentimento verificável dos pais, consentimento explícito, consentimento afirmativo, privacidade, direito do consumidor à privacidade, confidencialidade, precisão, relevância e utilização apropriada.

U.S. Legislation: Controlling the Assault of Non-Solicited Pornography and Marketing Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Health Insurance Portability and Accountability Act, Security Breach Notification Rule, Federal Trade Comission Act, Children's Online Privacy Protection Act, Controlling the Assault of Non-Solicited Pornography and Marketing Act, Financial Services Modernization Act, Gramm-Leach-Bliley Act,	**Legislação dos EUA**: Ato Legislativo sobre o Controle Infracional por Envio de Pornografia e Marketing não solicitados, Ato sobre Privacidade de Comunicações Eletrônicas, Lei sobre Fraude e Abuso de Computadores, Lei federal de Portabilidade e Responsabilidade de Seguro Saúde, Regra de Notificação de Violação de Segurança, Lei de Proteção à Privacidade Online das Crianças, Lei federal de Modernização dos Serviços Financeiros, Lei de Declaração de Crédito Justo.