Legislação no ambiente digital LGPD

Prof. Ana Carla Bliacheriene

Direito Digital

* Capitalismo informacional
  + Capitalismo baseado em informação capitalismo baseado em dados
* Dado é um atributo sem valor em sim quando ele adquire contexto falamos de informação, quando a informação define ou auxilia a tomada de uma decisão, falamos de conhecimento. Conhecimento com experiencias anteriores nos provem sabedoria
* Definição direito digital
  + Ramo do direito que rege as relações em ambientes virtuais
  + Todas as áreas do direito podem ter elações que perpassem pelo mundo virtual
* Direito digital Características
  + Celeridade
  + Dinamismo
  + Auto regulação
  + Poucas leis
  + Base Legal na prática costumeira
  + Uso de analogia
  + Uso de justiça multiportas
  + Se apoia nos princípios gerais do direito
* Direito digital Aplicações
  + Empresas Digitais
  + Provedores de acesso, de serviços e de conteúdos
  + E-business
  + Propriedade intelectual em mídias digitais
  + Marca em mídias digitais
  + Domínios
  + Software
  + Ferramentas de trabalho digitais
  + Isso de segurança da informação
  + Monitoramento
  + Trabalho Remoto
  + Assinatura digital
  + Documentos eletrônicos
  + Prova eletrônica
  + Biometria
  + Perícia Digital
  + Licitação Digital
  + Fintechs
  + Home Broker
  + Moedas digitais
  + Fisco Digitais
  + Justiça digital
  + Governo Digital
* Onde há gente há conflito, e onde há conflito tem de haver o direito
  + O modelo jurídico começa a se transformar para viabilizar o exercício da cidadania digital, seja através de ferramentas de peticionamento ou plebiscito online, ou ainda para garantir o direito de estar conectado à internet como um novo direito constitucional
  + Direito a estar conectado à internet é um direito fundamental que está na constituição
* LGPD -Lei Geral de Proteção de Dados pessoais
* Madrinhas cursos [tccsoftware@uspesalq.com](mailto:tccsoftware@uspesalq.com)
* Obrigação legal de recolher o mínimo de dado possível somente o necessário
* Definição de LGPO
  + Dado pessoal
    - Informação relacionada a pessoa natural identificada ou identificável
    - Isso quer dizer que ao pegar um dado puro não há infração a LGPD, porem a informação que é um dado relacionado deve atender a LGPD
    - O que a LGPD chama de dado é informação
    - **No contexto da LGPD Dado = Informação**
    - Fim Bloco 1
* ANPD 🡪 Autoridade Nacional de Proteção de Dados
* LGPD
  + Não proíbe a coleta de dados, o que ela regula é que o dono do dado saiba que o dado foi coletado, para que foi coletado, como será utilizado e por quem será utilizado. É necessário ter um fio condutor do uso desse dado e o detentor do dado deve ter a escolha de compartilhar ou não o dado
* Dados Pessoais
  + Informações que pode identificar diretamente ou indiretamente uma pessoa física
* LGPE não serve para identificar diretamente ou indiretamente uma pessoa física
* Privacidade = Direito Humano, garantido pela constituição
* Proteção de dados é um meio de se garantir a efetividade do exercício do direito humano a privacidade
* Não existe privacidade de dados, apenas proteção de dados ou sigilo de dados
* Direito Individual
  + Proteção do individuo em face do estado
* Direito de personalidade
  + Proteção do individuo em face de outros particulares, nas relações privadas
* LGPD
  + Proteger os direitos fundamentais a privacidade e o livre desenvolvimento da personalidade
  + Direito a proteção dos dados é um direito fundamental
* LGPD não é incompatível com a LAI (Lei de Acesso a Informação)
  + Transparência é a regra no setor publico
  + Ambas estão vigentes e devem ser obedecidas pelos órgãos públicos
* Dado pessoal
  + Informação relacionada a pessoa natural identificada ou identificável
* Dado Pessoal sensível
  + Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou vida sexual dado genético ou biométrico quando vinculado a uma pessoa natural

Fim Bloco 2

* Dado anonimizado
  + Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
* Pseudoanonimização
  + É o tratamento por meio do qual um dado perde a possibilidade de associação direta ou indireta, à um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em um ambiente controlado e seguro
* Tratamento
  + Toda operação realizada com dados pessoais
  + Qualquer verbo que se possa aplicar ao dado
  + Ex: coletar produzir, receber ...
* Controlador
  + Pessoa natural ou jurídica, de direito publico ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
* Operador
  + Pessoa natural ou jurídica de direito publico ou privado que realiza o tratamento de dados pessoais em nome do controlador
* Encarregado (DPO-Data Protection Officer)
  + Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados (ANPD)
* LGPD visa evitar
  + Discriminação
  + Manipulação
  + Supressão de direitos e liberdades
  + Vigilância e repressão
  + Vazamentos fraudes e outros crimes
  + Tem como um dos fundamentos o desenvolvimento tecnológico e a inovação
* Privacy By design
  + Como implementar os 7 princípios e garantir o exercício eficaz do direito individual e da personalidade a privacidade
    - Proativo e não reativo; preventivo e não corretivo
    - Privacidade como padrão (by default)
    - Privacidade incorporada ao design
    - Funcionalidade Total
    - Segurança de ponta a ponta
    - Visibilidade e transparência
    - Respeito pela privacidade do usuário
* Proativo e não reativo preventivo e não corretivo
  + Medidas técnicas e organizacionais
    - Garantir que a alta liderança esteja comprometida na disseminação de uma cultura forte de P&PD
    - Comunicar o programa de privacidade e educar os membros da organização no tema
    - Utilizar as ferramentas que a organização já adota de modo a garantir que o responsável pela P&PD em todos os assuntos envolvam o tratamento de dados pessoais, buscando, por exemplo, a minimização da coleta e uso desses dados
    - Avaliação de impacto à privacidade (PIA) realizada antes de qualquer novo tratamento de dados pessoais
    - Aplicar medidas técnicas de minimização, anonimização pseudoanonimização e práticas robustas de segurança da informação
* Privacidade por padrão
  + Privacidade deve ser a regra, o padrão sistemas e práticas da organização devem proteger os dados pessoais de foram automática sem necessidade de ação por parte do individuo
    - Configurações
      * Controles de privacidade automaticamente ativos em vez de dependerem de serem selecionados ou ativados pelo usuário
    - Anonimização
      * Implementação de controles para que o titular dos dados não seja reconhecido direta nem indiretamente seja pelo controlador atuando de modo independente ou em conjunto com outros agentes de tratamento
    - Limitação da coleta
      * Os dados coletados devem ser por padrão, apenas os estritamente necessários para cumprir a finalidade primaria informada no aviso de privacidade
    - Limitação de uso
      * O uso dos dados pessoais deve ser limitado ao cumprimento das finalidades já autorizadas pelo próprio titular ou previstas em lei, e isso deve ser garantido por meio de procedimentos e sistemas
* Funcionalidade Total
  + Medidas técnicas e organizacionais
    - Partir sempre do pressuposto que interesses legítimos podem coexistir: o da organização e o dos titulares de dados
    - Utilizar ferramentas de design que permita fazer workshops colaborativos para identificar, compreender e reunir múltiplos interesses, que à primeira vista podem parecer divergentes
    - Avaliar e equilibrar os interesses que possam parecer divergentes à primeira vista
    - Se as soluções propostas ameaçam a privacidade busque novas soluções e alternativas para atingir a funcionalidade total e os objetivos pretendidos lembrando que os riscos à privacidade dos usuários de produtos e serviços devem ser gerenciados de forma adequada
* Respeito pelo usuário
  + Medidas técnicas e organizacionais
    - Equilibrar os interesses legítimos da organização com o objetivo máximo de garantir a privacidade do usuário
    - Desenvolver aplicações, produtos e serviços privacy-friendly
    - Criar painéis de controle de privacidade para o usuário gerenciar o uso dos seus dados de forma granular
    - Implementar configurações de privacidade “Fortes” por padrão e informar aos usuários as consequências para a sua privacidade caso sejam modificadas
    - Criar avisos de privacidade com informações suficientes e adequadas para a coleta do consentimento livre, informado e inequívoco quando cabível
    - Criar mecanismos de transparência ativa durante a jornada do usuário para que sejam informados, novas atividades de tratamento de dados
    - Implementar mecanismos eficientes para que os titulares dos dados possam exercer seus direitos previstos em regulamentos de proteção de dados.
* Visibilidade e transparência
  + Ambiente logado com todas as informações disponíveis sobre o tratamento
  + Política de privacidade
  + Política e governança em privacidade
  + Manifesto
* Privacidade incorporada ao Desing
  + Medidas organizacionais
    - Documentações
    - Aplicação e comprovação desse princípio, pode ser feita por meio de documentos relacionados à arquitetura da solução, bem como outros documentos técnicos e de design da solução
    - Eles provam que as questões de privacidade foram incluídas no desenvolvimento desde a fase de ideação
* Segurança de ponta-a-ponta
  + A segurança da informação (dos dados pessoais) deve ser evada em consideração em todas as etapas, desde o desenho da solução e nos processos e procedimentos operacionais até a entrega da solução
    - Confidencialidade
      * Informações acessíveis somente para pessoas autorizadas
    - Disponibilidade
      * Veracidade, exatidão e completude das informações sem alterações não autorizadas
  + Devesa em profundidade
    - Políticas, procedimentos e conscientização
    - Segurança física
    - Segurança de perímetro
    - Segurança da rede interna
    - Segurança de Hosts/devices
    - Segurança da aplicação
    - Segurança de dados