ATIVIDADE ENADE - SPRINT 03 - AULA 05

Aluno: Luan Calazans 6°sem - Segurança Ofenssiva

QUESTÃO 1

A Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”, foi um marco na tipificação penal de crimes informáticos no Brasil. Entre outras disposições, a lei criminaliza a invasão de dispositivos eletrônicos sem autorização do titular, com o objetivo de obter, adulterar ou destruir dados.

Considerando o conteúdo dessa lei e seus impactos práticos,
avalie as seguintes situações:

I. Um funcionário invade o computador do colega de trabalho para copiar fotos pessoais, sem autorização.
II. Um pesquisador acessa seu próprio celular para verificar vulnerabilidades em aplicativos instalados.
III. Um atacante remoto invade o servidor de uma empresa para obter dados sigilosos de clientes.
IV. Um usuário acessa um site público do governo, sem realizar qualquer alteração ou acesso restrito.

Com base na Lei nº 12.737/2012, estão tipificadas como crime as situações:

A) Apenas I e III.

QUESTÃO 2

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet,

estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Entre seus fundamentos estão a proteção da privacidade, a neutralidade de rede e a guarda de registros.

Imagine a seguinte situação:
Um provedor de internet decide reduzir a velocidade de acesso de seus usuários quando utilizam plataformas de streaming, alegando que isso seria necessário para “proteger a rede”. Ao mesmo tempo, esse mesmo provedor coleta e armazena registros de navegação de usuários sem autorização judicial, disponibilizando-os a empresas de publicidade.

Com base no Marco Civil da Internet, assinale a alternativa que melhor caracteriza a conduta do provedor.

B) A prática de redução de velocidade viola o princípio da neutralidade de rede, e a coleta/compartilhamento de registros sem ordem judicial afronta a proteção da privacidade.

QUESTÃO 3

A LGPD (Lei nº 13.709/2018) dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade. Entre seus princípios estão a necessidade, a finalidade e a transparência no uso das informações.

Considere a situação:
Uma clínica médica coleta dados de seus pacientes por meio de formulário eletrônico. Além de informações essenciais para atendimento (nome, CPF, histórico de saúde), o formulário exige obrigatoriamente dados de convicção religiosa e filiação partidária, sem justificar a necessidade. Posteriormente, a clínica utiliza esses dados

para direcionar propaganda eleitoral de um candidato.

De acordo com a LGPD, essa prática é:

C) Irregular, pois envolve coleta excessiva de dados sensíveis sem finalidade clara, além de uso incompatível com a finalidade original.

QUESTÃO 4

Diversas leis brasileiras tratam de aspectos distintos da segurança e do uso da informação. Analise a coluna A (Leis) e relacione com a coluna B (focos principais de aplicação).

Coluna A – Leis

I. Lei nº 12.737/2012 (Lei Carolina Dieckmann)

II. Lei nº 12.965/2014 (Marco Civil da Internet)

III. Lei nº 13.709/2018 (LGPD)

Coluna B – Focos

1. Estabelece direitos, deveres e princípios para o uso da internet, incluindo a neutralidade de rede.
2. Tipifica crimes de invasão de dispositivos eletrônicos sem autorização.
3. Regula o tratamento de dados pessoais, estabelecendo princípios de proteção à privacidade.

A associação correta é:

A) I–2, II–1, III–3

QUESTÃO 5

Uma startup brasileira de tecnologia sofreu um incidente de segurança:

um invasor externo explorou falhas em um servidor de aplicação, obteve acesso a dados pessoais de milhares de clientes (incluindo CPF e endereço) e, em seguida, divulgou parte dessas informações em fóruns da internet.

Após o incidente, a imprensa noticiou o caso como "vazamento em massa", e órgãos reguladores iniciaram investigação. Durante a apuração, foi identificado que a empresa não possuía políticas claras de tratamento de dados, não havia registros adequados de consentimento dos titulares e não notificou a Autoridade Nacional de Proteção de Dados (ANPD) no prazo adequado.

Considerando as legislações brasileiras de segurança e privacidade digital, a lei aplicada de forma **mais abrangente e prioritária** nesse caso é:

C) Lei nº 13.709/2018 (LGPD), por regulamentar o tratamento de dados pessoais e prever sanções administrativas em caso de vazamento.

QUESTÃO 6

O artigo 19 da Lei nº 12.965/2014 (Marco Civil da Internet) estabelece que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para tornar indisponível o conteúdo apontado como infringente. O dispositivo foi concebido para equilibrar a liberdade de expressão e a proteção contra danos, evitando que os provedores atuem como censores privados e garantindo que a intervenção seja feita por decisão judicial.

Asserção (A): O provedor somente pode ser responsabilizado civilmente se, após ordem judicial específica, não tornar indisponível o

conteúdo apontado como infringente dentro do prazo e nos limites técnicos do seu serviço.

PORQUE

Razão (R): Em regra, a notificação extrajudicial do ofendido, contendo a identificação específica do material, é suficiente para gerar a responsabilidade do provedor pela manutenção do conteúdo.

Assinale a alternativa correta:

C) A é verdadeira, e R é falsa.

QUESTÃO 7

Um influenciador digital publica em uma rede social conteúdo ofensivo e difamatório contra uma empresa, resultando em danos à sua reputação. A empresa, sentindo-se prejudicada, envia uma notificação extrajudicial diretamente ao provedor da rede social solicitando a remoção imediata do conteúdo. O provedor, contudo, mantém a publicação no ar, alegando que só pode agir mediante ordem judicial.

Posteriormente, o caso chega ao Poder Judiciário, que determina a remoção do conteúdo. Durante o processo, discute-se se o provedor deveria ter sido responsabilizado desde a notificação inicial da empresa, sem necessidade de ordem judicial.

Com base no artigo 19 do Marco Civil da Internet e na jurisprudência do STF:

B) O provedor só poderia ser responsabilizado se descumprisse ordem judicial, exceto em situações de flagrante violação de direitos de difícil reversão, como conteúdo de ódio ou ilícito evidente.
nenhuma hipótese, já que não foi o autor direto do conteúdo.

QUESTÃO 8

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) prevê obrigações de segurança no tratamento de dados pessoais e estabelece regras para a comunicação de incidentes de segurança. Analise as afirmativas a seguir:

I. O controlador e o operador devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, como destruição, perda ou alteração.

II. O controlador é obrigado a comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, informando ao menos a descrição da natureza dos dados afetados.

III. O operador responde solidariamente com o controlador em qualquer incidente de segurança, ainda que não tenha descumprido instruções ou agido com culpa.

IV. A ausência de comunicação do incidente de segurança pela empresa pode gerar sanções administrativas previstas na LGPD, como advertência e multa, independentemente de outras esferas de responsabilização.

Está correto apenas o que se afirma em:

B) I, II e IV.

QUESTÃO 9

Um funcionário insatisfeito de uma empresa de comércio eletrônico

invadiu, sem autorização, o sistema interno da organização, obteve acesso a dados pessoais

de clientes (incluindo informações sensíveis) e os divulgou em fóruns da internet. A empresa só tomou ciência do incidente após clientes reportarem tentativas de fraude utilizando seus dados.

Considerando a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 13.709/2018 (LGPD), explique:

1. Como o ato do funcionário pode ser enquadrado penalmente, de acordo com a Lei nº 12.737/2012.
2. Quais são as obrigações da empresa diante da LGPD após a descoberta do incidente, especialmente em relação à comunicação da ocorrência e à responsabilização.

Sua resposta deve articular a aplicação **combinada** das duas normas, destacando a esfera penal e a administrativa.

O ato do funcionário pode ser enquadrado penalmente com base na Lei nº 12.737/2012 (Lei Carolina Dieckmann), que trata do crime de invasão de dispositivo informático. Ele acessou o sistema da empresa sem autorização e divulgou dados pessoais de clientes, o que caracteriza crime previsto no art. 154-A do Código Penal, com pena de reclusão e multa.
Já pela ótica da LGPD (Lei nº 13.709/2018), a empresa tem a responsabilidade administrativa de agir assim que toma conhecimento do incidente. Isso inclui comunicar a ANPD em até 72 horas e também informar os titulares dos dados afetados, explicando o que ocorreu e quais medidas estão sendo tomadas. Se essas obrigações não forem cumpridas, a empresa pode ser responsabilizada administrativamente, inclusive com aplicação de sanções como advertência ou multa.

QUESTÃO 10 – ENADE

Uma operadora de serviços digitais que atende em todo o território nacional registrou, no último trimestre, os seguintes incidentes de segurança:

- **Incidente A**: 250.000 contas de usuários tiveram senhas expostas por falha de configuração de banco de dados.
- **Incidente B**: 1.200 contas sofreram acessos não autorizados por ataque de força bruta, com uso fraudulento de dados de pagamento.
- **Incidente C**: 50.000 registros de clientes, contendo dados cadastrais, foram apagados indevidamente por erro de rotina de backup.

A empresa comunicou publicamente apenas o **Incidente B**, alegando que os outros não representariam risco ou dano relevante. Além disso, deixou de apresentar relatórios técnicos solicitados pelo Ministério Público e pela ANPD, sustentando que somente cumpriria determinação expressa do Poder Judiciário.

Com base na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e no Marco Civil da Internet (Lei nº 12.965/2014), responda de forma fundamentada:

1. Quais dos incidentes exigem comunicação obrigatória à ANPD e aos titulares, justificando sua resposta à luz do critério de “risco ou dano relevante” (art. 48 da LGPD).
2. Se a postura da empresa em só se submeter a ordem judicial é compatível com o regime de responsabilidade e de transparência imposto pelo Marco Civil da Internet.
3. Que tipo de sanções administrativas e responsabilizações civis podem recair sobre a empresa pela omissão ou pela recusa em cooperar com

autoridades competentes.

1) Comunicação obrigatória dos incidentes
Pela LGPD (art. 48) e pela regulamentação da ANPD, deve-se comunicar sempre que houver risco ou dano relevante aos titulares.

- Incidente A (senhas expostas): deve ser comunicado, pois envolve dados de autenticação em grande escala (250 mil usuários).

- Incidente B (fraude com dados de pagamento): deve ser comunicado, já que envolve dados financeiros e dano concreto (uso indevido).

- Incidente C (apagamento de 50 mil registros): em regra também deve ser comunicado, porque é perda de disponibilidade em larga escala e pode gerar prejuízos práticos aos clientes.

Portanto, os três incidentes pedem comunicação à ANPD e aos titulares, não só o B.

2) Postura da empresa frente às autoridades
A posição de “só cumprir ordem judicial” não é compatível com a LGPD nem com o Marco Civil. A ANPD e o Ministério Público têm legitimidade para requisitar informações sem necessidade de ordem judicial, e a empresa tem o dever de cooperação e transparência. Recusar-se a fornecer relatórios fere o princípio da prestação de contas e fragiliza a confiança com os usuários.

3) Possíveis sanções
Administrativas (LGPD e MCI): advertência, multa de até 2% do faturamento

(limitada a R$ 50 milhões por infração), bloqueio ou eliminação de dados, suspensão parcial ou total das atividades de tratamento, além da publicização da infração.

- Civis: obrigação de indenizar danos patrimoniais e morais, inclusive em ações coletivas.

- Reputacionais: desgaste de imagem, perda de confiança e risco de fiscalização mais severa no futuro.

Em resumo: a empresa deveria ter comunicado todos os incidentes, agir de forma transparente e colaborativa com ANPD e MP, e sua recusa pode gerar multas pesadas, restrições de atividade e processos civis por danos aos usuários.