**O caso: vazamento de dados da Record**

Em outubro de **2022**, a Record sofreu um *incidente de segurança / ataque hacker*, que afetou máquinas e servidores do ambiente tecnológico da empresa.

Alguns pontos do incidente:

* A área de Recursos Humanos (RH) da Record teve arquivos impactados, contendo dados pessoais e financeiros, dados de saúde, de dependentes, de filiação sindical, dados cadastrais de contato e comprovação de identidade etc.
* O vazamento também afetou **ex-funcionários**, ou seja, dados de pessoas que não estão mais sob vínculo direto ativo.
* A Record enviou comunicado aos funcionários e ex-funcionários informando sobre o incidente, dizendo que medidas de investigação já estavam sendo tomadas, apoio de consultoria externa foi acionado, e monitoramento da Deep Web para verificar possível exposição pública dos dados.

**1. Artigos da LGPD possivelmente violados**

Com base nesse caso, a Record pode ter violado os seguintes dispositivos da LGPD:

| **Artigo** | **Conteúdo relevante da lei** | **Como pode ter sido violado no caso da Record** |
| --- | --- | --- |
| **Art. 6º — Princípios** | Princípios como segurança, prevenção, transparência, responsabilização. | Não houve segurança suficiente para evitar o incidente; transparência foi feita posteriormente, mas princípio da prevenção foi violado. |
| **Art. 7º** | Hipóteses legais para o tratamento de dados pessoais. | Se dados foram mantidos além do necessário, ou usados para finalidades diferentes, ou sem base legal adequada, há violação. Dados de ex-funcionários podem estar sendo mantidos mais do que o permitido. |
| **Art. 9º** | Dados sensíveis — regras mais rigorosas para tratamento. | O caso menciona dados de **saúde**, que são dados sensíveis. Se não houve tratamento especial ou segurança reforçada, há infração. |
| **Art. 11º** | Tratamento por anonimização ou pseudonimização quando aplicável. | Se a empresa não anonimizou ou pseudonimizou dados onde seria apropriado, falha com esse artigo. |
| **Art. 12º, 13º, 14º** | Transparência para titulares: informação sobre coleta, finalidade, direito de acesso, correção etc. | Possivelmente a Record não informou com antecedência todos os titulares, ou não deixou claros os direitos, até que o incidente viesse a público. |
| **Art. 18º** | Direitos dos titulares — acesso, correção, eliminação, revogação de consentimento etc. | Titulares tem direito de saber quais dados foram afetados, pedir correção ou eliminação, etc. Se esses direitos não foram prontamente atendidos, há violação. |
| **Art. 46º** | Dever de adotar medidas técnicas e administrativas de segurança, prevenção de incidentes. | O vazamento indica falha nas medidas de segurança. |
| **Art. 48º** | Obrigação de comunicação do incidente à ANPD e aos titulares, quando houver risco ou dano relevante. | A Record comunicou aos funcionários (titulares) via RH, informou de investigação, etc. Também deverá ter comunicado à ANPD se o risco for relevante. Se não tiver feito, é violação. |
| **Art. 50º** | Relatórios de impacto à proteção de dados pessoais, registros das operações, documentação de incidentes. | Necessário registrar tudo: o que houve, quando, quem afetou, medidas tomadas. Caso isso não tenha sido bem documentado, há violação desse artigo. |

**2. Responsabilidades da empresa após descobrir o vazamento**

Com base na LGPD, essas são as responsabilidades que a Record (como controlador dos dados) tem após descoberta de um incidente como esse:

1. **Identificação e investigação técnica do incidente**  
   Determinar a origem, quais sistemas foram afetados, quais dados foram expostos, quantos titulares afetados, se dados sensíveis, se há risco de dano relevante ou uso indevido.
2. **Contenção e mitigação**  
   Interromper ou limitar a falha que permitiu o vazamento, corrigir vulnerabilidades, isolar sistemas comprometidos, etc.
3. **Notificação à ANPD**  
   Se o incidente puder acarretar risco ou dano relevante aos titulares, o controlador deve comunicar à Autoridade Nacional de Proteção de Dados, conforme o Art. 48 da LGPD.
4. **Notificação aos titulares dos dados afetados**  
   Avisar de forma clara, em prazo adequado, quais dados foram afetados, quais possíveis efeitos, orientações sobre o que eles podem fazer para se proteger (ex: monitorar contas, mudar senhas), medidas que a empresa tomou. No caso da Record, parece que houve uma comunicação aos funcionários/ex-funcionários.
5. **Registro e documentação do incidente**  
   Manter registros detalhados do incidente, inclusive data, hora, tipo de dados afetados, extensão, medidas de contenção e de mitigação, comunicações feitas, relatórios de impacto (se exigido) etc.
6. **Medidas corretivas e preventivas**  
   Rever políticas internas, segurança de sistemas, auditorias, treinamento de pessoal, reforçar controles de segurança da informação, criptografia, segregação de acesso etc.
7. **Cooperação com a ANPD e demais autoridades**  
   Disponibilizar documentos, informações, permitir auditoria, seguir determinações que vierem da ANPD.
8. **Avaliação de responsabilidade civil**  
   Caso os afetados sofram danos (morais ou materiais), a empresa poderá ser responsabilizada civilmente, inclusive em processos trabalhistas ou judiciais, especialmente por ex‐funcionários. No caso em questão, já há discussão de possibilidade de ações de empregados.
9. **Transparência pública**  
   Além de notificações aos titulares, fazer comunicação pública adequada (imprensa, canais internos) explicando o que ocorreu, para preservar confiança, reputação etc.
10. **Revogação ou eliminação dos dados, se aplicável**  
    Se for possível e necessário, eliminar dados desnecessários ou que não devam mais ser mantidos, especialmente de ex-funcionários, se não houver razão legal para conservá-los.

**3. Quais penalidades a ANPD poderia aplicar (Art. 52 LGPD)**

Com base no incidente e nas possíveis violações acima, a ANPD tem o poder de aplicar sanções previstas no Art. 52, de acordo com a gravidade, os riscos, a boa-fé, etc. Eis o que pode ser aplicado:

| **Tipo de sanção possível** | **Aplicabilidade no caso da Record** |
| --- | --- |
| **Advertência**, com determinação para correções | Sim, a ANPD pode emitir advertência indicando prazos para que Record implemente melhorias nos controles de segurança, governança de dados etc. |
| **Multa simples**, de até 2% do faturamento da empresa no Brasil no último exercício (excluídos tributos), limitada a R$ 50 milhões por infração | Dependendo do tamanho da Record (faturamento), esse tipo de multa pode alcançar valores elevados. Se for infração grave, com muitos titulares afetados, uso de dados sensíveis etc., esta multa pode ser considerável. |
| **Multa diária**, se não for cumprido o que foi determinado dentro dos prazos dados pela ANPD | Se for dada uma advertência ou ordem para corrigir algo, e a Record não cumprir, multa diária é possível. |
| **Publicização da infração**, ou seja, tornar público que houve violação e qual foi | Provavelmente será exigida; o incidente já é de conhecimento interno, mas a ANPD pode exigir que a empresa faça uma comunicação pública formal (ou reforçada) sobre o ocorrido. |
| **Bloqueio dos dados pessoais** relacionados à infração até regularização | A ANPD pode determinar que determinados dados afetados sejam bloqueados até que se comprove segurança, mitigação etc. |
| **Eliminação dos dados pessoais** relacionados à infração | Se os dados não forem necessários ou não tiverem base legal para manutenção, elimina-los pode ser uma exigência. |
| **Suspensão parcial do funcionamento do banco de dados** por até 6 meses (prorrogável) | Caso a infração envolva grave risco ou dano, a ANPD pode suspender o banco de dados usado para tratamento (ou parte dele) enquanto as correções não forem adequadas. |
| **Suspensão do exercício da atividade de tratamento** de dados pessoais relacionada à infração por até 6 meses (prorrogável) | Se for uma função essencial que esteja sendo mal gerida ou comprometedora, essa sanção pode ser aplicada. |
| **Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais** | Em casos extremos, se houver persistente descumprimento ou risco elevado, essa proibição pode ocorrer. |

Além disso, ao aplicar penalidades, a ANPD considera:

* a natureza, gravidade e extensão do dano aos titulares;
* se houve intenção ou culpa da empresa;
* se a empresa tomou medidas de prevenção ou mitigação antecipadas;
* o porte da empresa, sua capacidade econômica;
* se ocorreu reincidência;
* cooperação com a investigação.

Se quiser, posso estimar quais punições específicas a ANPD **deveria** aplicar ao caso da Record, com base nas informações públicas — e também mostrar decisões semelhantes para comparação. Você quer isso?