**Respostas com fundamentação na LGPD (Lei Geral de Proteção de Dados - Lei nº 13.709/2018):**

**a) Respostas da empresa em acordo com a LGPD**

**Nenhuma** das respostas da Trevixel Sistemas está em conformidade com a LGPD.

**b) Respostas da empresa em desacordo com a LGPD**

Todas as respostas da empresa violam a LGPD:

1. **Cobrança de taxa para exclusão de dados**
   * **Violação**: O Art. 18, VI, da LGPD garante ao titular o direito à exclusão dos dados sem custo, exceto em casos de tratamento lícito e necessidade de conservação (Art. 16). A empresa não pode cobrar para cumprir um direito previsto em lei.

“§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.”

* + **Fundamentação**: Art. 18, VI, e Art. 16 da LGPD (BRASIL, 2018).

1. **Negativa de portabilidade**
   * **Violação**: O Art. 18, V, assegura ao titular a portabilidade dos dados a outro fornecedor de serviço, mediante requisição expressa. A empresa não pode se recusar a fornecer os dados em formato estruturado.

**“§** 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador**.”**

* + **Fundamentação**: Art. 18, V, da LGPD (BRASIL, 2018).

1. **Recusa de acesso aos dados por "segurança"**
   * **Violação**: O Art. 18, I e II, garante ao titular o direito de acessar seus dados e obter informações sobre seu tratamento. A empresa deve fornecer esses dados, exceto em casos de segredo industrial (Art. 9º, § 2º), que não se aplica aqui.

**“**Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados**;**

“

* + **Fundamentação**: Art. 18, I e II, e Art. 9º, § 2º, da LGPD (BRASIL, 2018).

**c) Direitos que Kael pode exigir**

Kael pode exigir, com base no **Art. 18 da LGPD**:

1. **Acesso aos dados** (Art. 18, I): Obter cópia dos dados armazenados pela empresa.
2. **Correção ou exclusão** (Art. 18, VI): Solicitar a eliminação gratuita de seus dados pessoais.
3. **Portabilidade** (Art. 18, V): Transferir seus dados para outra empresa.
4. **Informação sobre o tratamento** (Art. 18, II): Saber como seus dados são utilizados.

**Fundamentação**: Art. 18 da LGPD (BRASIL, 2018).

**d) Cuidados para profissionais de TI**

Os profissionais devem seguir os **princípios da LGPD (Art. 6º)**, especialmente:

1. **Finalidade**: Coletar dados apenas para propósitos legítimos (Art. 6º, I).

**“**Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades**;”**

1. **Transparência**: Informar titulares sobre o uso dos dados (Art. 6º, VI).

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

1. **Segurança**: Adotar medidas técnicas para proteger os dados (Art. 46).

**“**Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito**.”**

1. **Não discriminação**: Não condicionar serviços ao fornecimento de dados excessivos (Art. 6º, III).

**“**III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados**;”**

**Fundamentação**: Art. 6º e Art. 46 da LGPD (BRASIL, 2018).

**e) Dados sensíveis no caso**

Nenhum dos dados fornecidos por Kael (nome, CPF, e-mail, etc.) é considerado **dado sensível** pela LGPD. Dados sensíveis são definidos no **Art. 5º, II**, como informações sobre origem racial, saúde, orientação sexual, etc.

“Art. 5º Para os fins desta Lei, considera-se:

II - 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 à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;”

**Fundamentação**: Art. 5º, II, da LGPD (BRASIL, 2018).

**Referências Bibliográficas (ABNT):**

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: [07 de Abril de 2025].

Bônus:

Existe um jogo da empresa Ubisoft em que o tema central gira em torno da vigilância, privacidade e do uso (e abuso) de dados pessoais por grandes corporações e governos. A DedSec, organização da qual o protagonista Marcus faz parte, luta justamente contra o sistema ctOS 2.0, uma rede de coleta de dados que monitora e manipula a vida das pessoas.

Gosto de traçar paralelos entre a vida real e a fictícia, já que ambas se inspiram entre si.

Watch Dogs 2 apresenta uma sociedade onde tudo é interligado e monitorado — desde câmeras até dados bancários e perfis de redes sociais. Esse cenário é uma crítica ao uso desenfreado de tecnologia sem regulação.

A GDPR, implementada em 2018 na União Europeia, surgiu como resposta a esse tipo de preocupação, estabelecendo regras claras sobre como dados pessoais devem ser coletados, armazenados e usados.

A LGPD, inspirada na GDPR, entrou em vigor no Brasil em 2020, com o mesmo espírito de proteger os direitos do cidadão frente ao avanço tecnológico e à coleta massiva de dados.

No jogo, as pessoas são monitoradas sem consentimento real. Empresas como a Blume usam dados para manipular opiniões e comportamentos, o que ecoa casos reais como o escândalo da Cambridge Analytica.

A LGPD exige consentimento claro e informado para o uso de dados sensíveis — algo que no mundo de Watch Dogs 2 simplesmente não existe. A crítica é justamente essa ausência de controle por parte do indivíduo.

O ctOS 2.0 é uma ferramenta de vigilância em massa, o que levanta questões éticas semelhantes às que inspiraram a criação de leis como a GDPR.

A LGPD tenta equilibrar o poder, criando a ANPD (Autoridade Nacional de Proteção de Dados) para fiscalizar e proteger os cidadãos.

A DedSec representa uma forma de resistência civil a esse sistema abusivo. Enquanto a LGPD oferece uma solução legal e institucional, o jogo mostra a luta pela privacidade de forma mais direta, rebelde e radical.

Esse contraste pode gerar discussões interessantes sobre até que ponto confiar apenas na legislação é suficiente, ou se movimentos sociais (inclusive virtuais) são necessários para pressionar por mudanças reais. 