

DADOS PESSOAIS E PRIVACIDADE UMA ANÁLISE CONCEITUAL E ESTRUTURAL À LUZ DA LGPD

Você tem certeza de que sabe reconhecer um dado pessoal?

A maioria dos profissionais acredita que CPF, RG e e-mail são dados pessoais.

Mas poucos percebem que uma gravação de voz, um GPS, um desenho infantil ou até uma ata de reunião também podem ser dados pessoais.

O problema é que esse erro de interpretação gera riscos jurídicos enormes

Dados pessoais significam qualquer informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); é adaptada uma definição ampla, a fim de abranger todas as informações que possam estar relacionadas com um indivíduo.

Dados pessoais seja tão geral quanto possível, de modo a incluir todas as informações relativas a uma pessoa identificável, levando em conta que o intuito é proteger os direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à privacidade.

Poderíamos ter uma série de situações em que os direitos dos indivíduos não estão em risco, e as mesmas regras que deixariam os indivíduos privados da proteção dos seus direitos.

Apesar do conceito amplo de “dados pessoais” e de “tratamento” contido na LGPD, o simples fato de uma determinada situação ser considerada como “tratamento de dados pessoais” não determina a aplicação da lei. Mesmo quando está envolvendo o tratamento de dados pessoais, nem todas as regras nela contidas podem ser aplicadas. Devemos encontrar o equilíbrio adequado entre a proteção dos direitos das pessoas, e por outro lado, os interesses legítimos dos responsáveis pelo tratamento dos dados, de terceiros e o interesse público que possa estar presente.

Devemos evitar a interpretação restrita e única de dados pessoal sem olhar o contexto do tratamento e o que ele representa. Isso pelo fato de dados pessoal: PEC 17/19, que incorporou a CF o direito fundamental e garantia à proteção.

Devemos ter um olhar com definição que seja suficientemente ampla para poder antecipar evoluções e abranger todas as “zonas sombrias” – Riscos

Quatro elementos principais, que devemos analisar separadamente para garantirmos privacidade e proteção.

1. Qualquer operação;
2. Relacionada a;
3. Identificada ou identificável;
4. Pessoa natural.

1º PRIMEIRO ELEMENTO: “QUALQUER INFORMAÇÃO

*A LGPD não protege documentos.
Ela protege pessoas.*

Conceito amplo de dados pessoais. Esta formulação exige uma interpretação ampla.

Abrange informações “objetivas”, também inclui informações, opiniões ou avaliações “subjetivas”.
Para que as informações sejam ‘dados pessoais’, não é necessário que sejam verdadeiras ou comprovadas, na verdade, as regras de proteção de dados já prevêm a possibilidade das informações serem incorretas e preveem o direito do titular dos dados de corrigi-las e de contestá-las. O termo “dados pessoais” inclui informações relativas à vida privada e familiar do indivíduo, mas também informações relativas a qualquer tipo de atividade desenvolvida pelo indivíduo, como às relações de trabalho ou ao comportamento económico ou social do indivíduo. Inclui, portanto, informações sobre indivíduos, independentemente da posição ou capacidade dessas pessoas (como consumidor, paciente, funcionário, cliente, etc.).

Exemplo nº 1: Hábitos e práticas profissionais:

Informações sobre prescrição de medicamentos (por exemplo, número de identificação do medicamento, nome do medicamento, dosagem do medicamento, fabricante, preço de venda, novo ou não, motivos de uso, motivos para não pedido de substituição, nome e sobrenome do médico, número de telefone, etc.), seja na forma de prescrição individual ou na forma de padrões discernidos a partir de uma série de prescrições, podem ser considerados dados pessoais do médico que prescreve o medicamento, *mesmo que o paciente seja anônimo*. Assim, fornecer informações sobre receitas prescritas por médicos identificados ou identificáveis a fabricantes de medicamentos sujeitos a receita médica constitui uma comunicação de dados pessoais a terceiros destinatários na ação do médico

Considerando o formato ou forma em que essa informação está contida, o conceito de dados pessoais inclui a informação disponível sob qualquer forma, seja ela alfabética, numérica, gráfica, fotográfica ou acústica, por exemplo. Inclui informações mantidas em papel, bem como informações armazenadas na memória do computador por meio de código binário ou em fita de vídeo, por exemplo.

Em particular, os dados de som e de imagem são considerados dados pessoais deste ponto de vista, na medida em que possam representar informações sobre um indivíduo. *“Dada a importância da evolução em curso, no quadro da sociedade da informação, das técnicas utilizadas para capturar, transmitir, manipular, gravar, armazenar ou comunicar dados de som e de imagem relativos a pessoas singulares”*

Posso ter uma gravação totalmente anônima, porém o simples fato de identificação do médico na hora de salvar o arquivo, já identifico um dado pessoal do médico e dependendo da tecnologia podemos identificar o dado (doença) do paciente, que estava anônimo.

Exemplo nº 2: Central Telefônica:

Na central telefônica, onde a voz do titular dando instruções a central é gravada em fita, essas instruções gravadas devem ser consideradas dados pessoais.

Exemplo nº 3: Vídeo Monitoramento:

As imagens de indivíduos capturadas por um sistema de CFTV podem ser dados pessoais na medida em que os indivíduos sejam reconhecíveis.

Se houver possibilidade razoável de identificação, trata-se de dado pessoal.

Exemplo nº 4: Desenho de Uma Criança:

Como resultado de um teste neuropsiquiátrico realizado a uma menina no âmbito de um processo judicial sobre a sua guarda, é apresentado um desenho feito por ela em representação da sua família. O desenho fornece informações sobre o humor da menina e o que ela sente em relação aos diferentes membros de sua família. Como tal, podem ser considerados “dados pessoais”.

O desenho revelará, de fato, informações relativas à criança (o seu estado de saúde do ponto de vista psiquiátrico) e também, por exemplo, sobre o comportamento do pai ou da mãe. Como resultado, os pais, nesse caso, poderão exercer o seu direito de acesso a esta informação específica.

2º SEGUNDO ELEMENTO: “RELACIONADO COM”

O dado não nasce pessoal.

Ele se torna pessoal quando consegue representar alguém.

Este alicerce da definição é crucial, pois é muito importante descobrir com precisão quais são as relações/ligações que importam e como distingui-las. Em muitas situações, esta relação pode ser facilmente estabelecida. Por exemplo, os dados registados no ficheiro individual no RH estão claramente “relacionados” com a situação da pessoa como empregado. O mesmo ocorre com os dados sobre os resultados do exame médico de um paciente contidos em seus registros médicos, ou a imagem de uma pessoa filmada em uma entrevista em vídeo dessa pessoa.

No entanto, podem ser mencionadas várias outras situações em que nem sempre é tão evidente como nos casos anteriores determinar que a informação “se refere” a um indivíduo.

Exemplo nº 5: Valor de uma Casa

Em termos gerais, pode-se considerar que a informação “se relaciona” com um indivíduo quando se trata desse indivíduo. O valor de uma determinada casa é uma informação sobre o objeto. É evidente que as regras de proteção de dados não serão aplicáveis quando esta informação for utilizada apenas para ilustrar o preço do imóvel. No entanto, em determinadas circunstâncias, essas informações também deverão ser consideradas dados pessoais. Com efeito, a casa é património de um proprietário, que será, portanto, utilizado para determinar a extensão da obrigação desta pessoa de pagar alguns impostos, por exemplo. Neste contexto, será indiscutível que tais informações devem ser consideradas dados pessoais.

Exemplo nº 6: Registro de Serviço de Carro

O registro de serviço de um carro mantido por um mecânico ou oficina contém informações sobre o carro, quilometragem, datas de verificações de serviço, problemas técnicos e condições do material. Esta informação está associada no registro a uma matrícula e a um número de motor, que por sua vez pode ser ligado ao proprietário. Quando a oficina estabelece uma ligação entre o veículo e o proprietário, para efeitos de faturamento, a informação será “relativa” ao proprietário ou ao condutor. Se a ligação for feita com o mecânico que trabalhou no carro com o objetivo de apurar sua produtividade, essa informação também será pessoal e “relativa” ao mecânico.

À questão de saber quando é que a informação pode ser considerada "relativa" a uma pessoa. Pode-se salientar que, para considerar que os dados “relacionam” a um indivíduo, é necessário um elemento de “**conteúdo**” OU um elemento de “**finalidade**” OU um elemento de “**resultado**”. " Um elemento deve estar presente.

- “**conteúdo**”: é fornecida informação sobre uma determinada pessoa, independentemente de qualquer finalidade por parte do responsável pelo tratamento ou de terceiros, ou o impacto dessas informações sobre o titular dos dados.
- “**finalidade - propósito**”: Tratar de determinada forma ou influenciar o estado ou comportamento de um indivíduo.

Exemplo nº 7: Registro de chamadas para um telefone

O registro de chamadas de um telefone dentro do escritório de uma empresa fornece informações sobre as chamadas feitas daquele telefone conectado a uma determinada linha. Essas informações podem ser relacionadas com diferentes assuntos. Por um lado, a linha foi disponibilizada à empresa, estando a empresa contratualmente obrigada a pagar essas chamadas. O aparelho telefónico fica sob o controle de um determinado funcionário durante o horário de trabalho e as ligações devem ser feitas por ele. O registro de chamadas também pode fornecer informações sobre a pessoa que foi chamada.

O telefone também pode ser utilizado por qualquer pessoa autorizada a entrar nas instalações na ausência do funcionário (por exemplo, pelo pessoal de limpeza). Para diferentes fins, a informação sobre a utilização desse aparelho telefónico pode ser relativa à empresa, ao funcionário ou ao pessoal de limpeza (por exemplo, para verificar a hora em que o pessoal de limpeza sai do local de trabalho, pois deve confirmar por telefone a que horas saem antes de trancar as instalações). Vemos que o conceito de dados pessoais se estende aqui tanto às chamadas efetuadas como às recebidas, na medida em que todas contêm informações relativas à vida privada, às relações sociais e às comunicações das pessoas.

- “**resultado**”. Apesar da ausência de um elemento de “conteúdo” ou de “finalidade”, os dados podem ser considerados como “relativos” a um indivíduo porque a sua utilização é suscetível de ter um impacto nos direitos e interesses de uma determinada pessoa, tendo em conta todas as circunstâncias que rodeiam o caso.

Deve-se notar que não é necessário que o resultado potencial seja de grande impacto. É suficiente que o indivíduo possa ser tratado de forma diferente de outras pessoas como resultado do tratamento de tais dados.

Exemplo nº 8: GPS dos carros para otimizar o serviço com impacto nos motoristas.

Um sistema de localização por satélite é montado por uma empresa que permite determinar em tempo real a posição dos carros disponíveis. O objetivo do tratamento é prestar um melhor serviço e poupar combustível, atribuindo a cada cliente que solicita um carro mais próximo da moradia do cliente. Estritamente falando, os dados necessários para esse sistema são dados relativos aos automóveis e não aos condutores. O objetivo do tratamento não é avaliar o desempenho dos motoristas, por exemplo através da otimização dos seus itinerários.

No entanto, o sistema permite monitorizar o desempenho dos motoristas e verificar se respeitam os limites de velocidade, procuram rotas adequadas, estão ao volante ou descansam ao ar livre, etc. pode considerar-se que os dados também dizem respeito a pessoas singulares. O tratamento deverá estar sujeito às regras de proteção de dados.

Estes três elementos (conteúdo, finalidade, resultado) devem ser considerados como condições alternativas e não cumulativas.

Quando um está presente, não há necessidade de que os outros elementos estejam presentes para considerar que a informação se refere ao indivíduo. A questão de saber se os dados dizem respeito a uma determinada pessoa é algo que deve ser respondido para cada item de dados específico com base nos seus próprios méritos.

Exemplo nº 9: Ata de reunião.

Um exemplo da necessidade de realizar a análise prévia de cada informação separadamente diz respeito às informações contidas na ata de uma reunião, registrando normalmente a presença dos participantes T, C e S; as declarações de T e C; e um relatório dos trabalhos sobre determinados temas resumidos pelo autor da ata, S. Como dados pessoais relativos a T só se pode considerar a informação de que este participou na reunião em determinado horário e local, e de que fez determinadas declarações.

A presença na reunião de G, suas declarações e os procedimentos sobre um assunto resumido por S NÃO são dados pessoais relativos a T. Isto acontece mesmo que esta informação esteja contida no mesmo documento, e mesmo que tenha sido T quem desencadeou o assunto a ser discutido na reunião. Está, portanto, excluído do direito de acesso de T aos seus próprios dados pessoais. Se em que medida essas informações podem ser consideradas dados pessoais de G e S terão de ser determinados separadamente, utilizando a análise descrita anteriormente.

3. TERCEIRO ELEMENTO: “IDENTIFICADO OU IDENTIFICÁVEL”

Em termos gerais, uma pessoa singular pode ser considerada “identificada” quando, dentro de um grupo de pessoas, se “distingue” de todos os outros membros do grupo. Assim, a pessoa singular é “identificável” quando, embora ainda não tenha sido identificada, é possível fazê-lo.

A identificação é normalmente conseguida através de informações específicas que podemos chamar de “**identificadores**” e que mantêm uma relação particularmente privilegiada e próxima com o indivíduo em particular.

Exemplos são os sinais exteriores da aparência dessa pessoa, como a altura, a cor do cabelo, o vestuário, etc., ou uma qualidade da pessoa que não pode ser imediatamente percebida, como uma profissão, uma função, um nome, etc. ”

Uma pessoa pode ser identificada diretamente pelo nome ou indiretamente, através de um número de telefone, de uma matrícula, automóvel, de um número de segurança social, de um número de passaporte ou através de uma combinação de critérios significativos que permitam o seu reconhecimento através da restrição do grupo a que pertence (idade, profissão, local de residência, etc.).”

Um apelido muito comum não será suficiente para identificar alguém, ou seja, para isolar alguém de toda a população de um país, embora seja provável que consiga a identificação de um aluno em uma sala de aula. Mesmo informações auxiliares, como "o homem de terno preto" podem identificar alguém entre outras mais em pé num semáforo, pelo que a questão de saber se a pessoa a quem a informação se refere está ou não identificada depende das circunstâncias do caso (proximidade).

Para determinar esta identidade, o nome da pessoa tem por vezes de ser combinado com outras informações (data de nascimento, nomes dos pais, morada ou fotografia do rosto) para evitar confusão entre essa pessoa e possíveis homónimos.

O nome também pode ser o ponto de partida para obter informações sobre o local onde a pessoa vive ou pode ser encontrada, pode também fornecer informações sobre as pessoas da sua família (através do apelido) e sobre uma série de diferentes relações sociais associadas a esse nome (registros educacionais, registos médicos, contas bancárias).

Pode até ser possível saber a aparência da pessoa se a sua fotografia estiver associada a esse nome. Todas essas novas informações vinculadas ao nome podem permitir que alguém se aproxime do indivíduo de carne e osso e, portanto, através dos identificadores, a informação original é associada a uma pessoa física que pode ser distinguida de outros indivíduos.

No que diz respeito às pessoas “indiretamente” identificadas ou identificáveis, esta categoria refere-se normalmente ao fenómeno das “combinações únicas”, sejam elas pequenas ou grandes. Nos casos em que a extensão dos identificadores disponíveis não permite que alguém destaque uma pessoa específica, essa pessoa ainda pode ser “identificável” porque essa informação combinada com outras informações (sejam estas últimas retidas pelo controlador de dados ou não) permitirá que o indivíduo se distinga dos outros.

Exemplo nº 10: Informações fragmentárias na imprensa

São publicadas informações sobre um antigo caso criminal que ganhou muita atenção do público no passado. Na presente publicação não há nenhum dos identificadores tradicionais fornecidos, especialmente nenhum nome ou data de nascimento de qualquer pessoa envolvida. Não parece

excessivamente difícil obter informações adicionais que permitam descobrir quem são as principais pessoas envolvidas, por exemplo, consultando jornais do período relevante.

Na verdade, pode-se presumir que não é completamente improvável que alguém tome tais medidas (como consultar jornais antigos) que muito provavelmente forneceriam nomes e outros identificadores para as pessoas referidas no exemplo. Parece, portanto, justificado considerar as informações constantes do exemplo dado como sendo «informações sobre pessoas identificáveis» e, como tal, «dados pessoais».

Na Web, as ferramentas de vigilância de tráfego facilitam a identificação do comportamento de uma máquina e, por trás da máquina, do seu usuário. Assim, a personalidade do indivíduo é montada para lhe atribuir determinadas decisões.

Sem sequer perguntar sobre o nome e endereço do indivíduo, é possível categorizá-lo com base em critérios socioeconômicos, psicológicos, filosóficos ou outros e atribuir-lhe determinadas decisões, uma vez que o ponto de contato do indivíduo (um computador) já não exige necessariamente a divulgação da sua identidade em sentido estrito. Por outras palavras, a possibilidade de identificar um indivíduo já não significa necessariamente a capacidade de descobrir o seu nome.

Exemplo nº 11: Asilo

a) - Os requerentes de asilo que escondem os seus nomes verdadeiros numa instituição de acolhimento receberam um número de código para fins administrativos. Esse número servirá de identificador, para que lhe sejam anexadas diferentes informações relativas à permanência do requerente de asilo na instituição e, através de fotografia ou outros indicadores biométricos, o número de código terá uma identificação próxima e imediata ligação à pessoa física, permitindo assim distingui-lo de outros requerentes de asilo e atribuir-lhe diferentes informações, que passarão então a referir-se a uma pessoa singular “identificada”.

b) - Os dados se destinarem a ser armazenados durante um mês, a identificação pode não ser possível durante a “vida útil” da informação. No entanto, caso se destinem a ser conservados durante 10 anos, o responsável pelo tratamento deverá considerar a possibilidade de identificação que poderá ocorrer também no nono ano da sua vida, e que poderá torná-los dados pessoais nesse momento. O sistema deverá ser capaz de se adaptar a estes desenvolvimentos à medida que estes ocorrem e de incorporar oportunamente as medidas técnicas e organizacionais adequadas.

Exemplo nº 12: Publicação de placas de raios X juntamente com o primeiro nome do paciente

O Raio X de uma senhora foi publicada numa revista científica, juntamente com o primeiro nome da senhora, o que era muito incomum. O primeiro nome da pessoa, aliado ao conhecimento dos seus familiares ou conhecidos de que ela sofria de uma determinada doença, tornava a pessoa identificável por várias pessoas, e a placa de raios X seria então considerada como dado pessoal.

Exemplo nº 13: Dados de pesquisa farmacêutica

Hospitais ou médicos individuais transferem dados dos registros médicos de seus pacientes para uma empresa para fins de pesquisa médica. Não são utilizados nomes dos pacientes, mas apenas números de série atribuídos aleatoriamente a cada caso clínico, a fim de garantir coerência e evitar confusão com informações sobre diferentes pacientes.

Os nomes dos pacientes ficam exclusivamente na posse dos respectivos médicos, vinculados ao sigilo médico. Os dados não contêm quaisquer informações adicionais que possibilitem a identificação dos pacientes através da sua combinação. Além disso, todas as outras medidas foram tomadas para evitar que os titulares dos dados sejam identificados ou se tornem identificáveis, sejam eles legais, técnicos ou organizacionais.

Nestas circunstâncias, A Agência de Proteção de Dados pode considerar que no tratamento efetuado pela empresa farmacêutica não existem meios que tornem provável a sua utilização razoável para identificar os titulares dos dados.

- *Na verdade, argumentar que os indivíduos não são identificáveis, quando o objetivo do tratamento é precisamente identificá-los, seria uma pura contradição em termos.*

Exemplo nº 14: CFTV

Isto é particularmente relevante no contexto da CFTV, onde os responsáveis pelo tratamento argumentam frequentemente que a identificação só aconteceria numa pequena percentagem do material recolhido e, portanto, antes que a identificação, nestes poucos casos, realmente ocorra, nenhum dado pessoal é tratado. Como o *objetivo da CFTV é, no entanto, identificar as pessoas que podem ser vistas nas imagens em todos os casos em que tal identificação seja considerada necessária* pelo responsável pelo tratamento, todo o tratamento enquanto tal deve ser considerado como um tratamento de dados sobre pessoas identificáveis, mesmo que algumas pessoas registadas não sejam identificáveis na prática.

Exemplo nº 15: endereços IP dinâmicos

Os endereços IP como dados relativos a uma pessoa identificável. "Os fornecedores de acesso à Internet e os gestores de redes locais podem, através de meios razoáveis, identificar os usuários da Internet aos quais atribuíram endereços IP, uma vez que normalmente "registam" sistematicamente num ficheiro a data, a hora, a duração e o endereço IP dinâmico dados ao usuário.

O mesmo se pode dizer dos fornecedores de serviços de Internet que mantêm um "diário de bordo" no servidor HTTP. Nestes casos não há dúvida de que se pode falar de dados pessoais.

Especialmente nos casos em que o tratamento de endereços IP é efetuado com o objetivo de identificar os usuários do computador (por exemplo, pelos titulares de direitos de autor, a fim de processar os utilizadores de computador por violação de direitos de propriedade intelectual).

Exemplo nº 16: Danos causados por Grafite

Os veículos de passageiros de uma empresa de transporte sofrem danos repetidos com pichações. Para avaliar os danos e facilitar o exercício de ações judiciais contra seus autores, a empresa organiza um cadastro contendo informações sobre as circunstâncias do dano, bem como imagens dos itens danificados e das "etiquetas" ou "assinatura" do autor. No momento da inscrição da informação no

registro, não se conhecem os autores do dano nem a quem corresponde a “assinatura”. *Pode muito bem acontecer que nunca seja conhecido.*

No entanto, a finalidade do tratamento é precisamente identificar as pessoas a quem a informação se refere como autores do dano, para poder exercer ações judiciais contra elas. Tal tratamento faz sentido se o responsável pelo tratamento dos dados considerar “razoavelmente provável” que um dia haverá meios de identificar o indivíduo. As informações contidas nas imagens devem ser consideradas como relativas a indivíduos “identificáveis”, as informações constantes do registro como “dados pessoais” e o tratamento deve estar sujeito às regras de proteção de dados, que permitem esse tratamento como legítimo em determinadas circunstâncias e sujeito a certas salvaguardas.

A implementação de medidas técnicas e organizacionais adequadas e de última geração para proteger os dados contra a identificação pode fazer a diferença para considerar que as pessoas não são identificáveis, tendo em conta *todos os meios que possam ser razoavelmente utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa* para identificar os indivíduos.

Exemplo nº 17: Dados não agregados para estatísticas

Um exemplo para ilustrar a importância de ter em conta todas as circunstâncias para avaliar se os meios de identificação são “prováveis razoavelmente” de serem utilizados poderia ser as informações pessoais processadas pela empresa de estatística, onde, numa determinada fase, a informação é mantida de forma não agregada e diz respeito a indivíduos específicos, mas estes são designados com um código em vez de um nome (por exemplo, o indivíduo com o código X1234 bebe um copo de vinho mais de 3 vezes por semana).

A empresa de estatística mantém separadamente a chave destes códigos (a lista que associa os códigos aos nomes das pessoas). Essa chave pode ser considerada **“razoavelmente utilizada”** pela empresa de estatística e, portanto, o conjunto de informações relacionadas com indivíduos pode ser considerado como dados pessoais e deve estar sujeito às regras de proteção de dados da empresa. Agora, podemos imaginar que uma lista com dados sobre os hábitos de consumo de vinho dos consumidores seja transferida para a organização de produtores de vinho, a fim de lhes permitir apoiar a sua posição pública em números estatísticos. Para determinar se essa lista de informações ainda constitui dados pessoais, deverá avaliar se os consumidores individuais de vinho podem ser identificados *“tendo em conta todos os meios serem razoavelmente utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa”*.

Se os códigos utilizados forem únicos para cada pessoa específica, o risco de identificação ocorre sempre que for possível obter acesso à chave utilizada para a criptografia. Por conseguinte, os riscos de uma pirataria externa, a probabilidade de alguém dentro da organização do remetente ter acesso ao seu sigilo profissional e fornecer a chave e a viabilidade da identificação indireta são fatores a se levar conta para determinar se as pessoas podem ser identificadas *tendo em conta todos os meios que possam ser razoavelmente utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa* e, portanto, se as informações devem ser consideradas como “dados pessoais”. Se assim for, serão aplicadas as regras de proteção de dados.

Uma questão diferente é que essas regras de proteção de dados poderiam ter em conta se os riscos para os indivíduos são reduzidos e sujeitar o tratamento a condições mais ou menos rigorosas, com base na **“flexibilidade”** permitida pelas regras.

Se, pelo contrário, os códigos não forem únicos, mas o mesmo número de código (por exemplo, "123") for utilizado para designar indivíduos em cidades diferentes e para dados de anos diferentes (distinguindo apenas um determinado indivíduo dentro de um ano e dentro da amostra na mesma cidade), o controlador ou terceiro só poderia identificar um indivíduo específico se soubesse a que ano e a que cidade os dados se referem. Se estas informações adicionais tiverem desaparecido e não for provável que sejam razoavelmente recuperadas, poderá considerar-se que as informações não se referem a pessoas identificáveis e não estariam sujeitas às regras de proteção de dados.

Esse tipo de dados é comumente usado em ensaios clínicos com medicamentos. O profissional médico/pesquisador (*"investigador"*) que testa os medicamentos coleta as informações sobre os resultados clínicos de cada paciente, atribuindo-lhe um código. O investigador fornece a informação à empresa farmacêutica ou outras partes envolvidas (*"patrocinadores"*) apenas nesta forma codificada, uma vez que estão interessados apenas em informação bioestatística. Porém, o investigador mantém separadamente uma chave associando este código a informações comuns para identificar os pacientes de forma separada. Para proteger a saúde dos pacientes caso os medicamentos representem perigos, o investigador é obrigado a guardar esta chave, para que os pacientes individuais possam ser identificados em caso de necessidade e receber tratamento adequado. Neste caso, a identificação das pessoas singulares (para aplicar o tratamento adequado em caso de necessidade) é uma das finalidades do tratamento dos dados codificados com chave, não é apenas algo que *pode* acontecer, mas sim como algo que *deve*

Dados anônimos

Mais uma vez, a avaliação se os dados permitem a identificação de um indivíduo e se a informação pode ser considerada anônima ou não depende das circunstâncias e de uma análise caso a caso. A análise deverá ser realizada com especial referência na medida em que os meios possam ser razoavelmente utilizados para a identificação. Isto é particularmente relevante no caso da informação estatística, onde, apesar da informação poder ser apresentada como dados agregados, a amostra original não é suficientemente grande e outras informações podem permitir a identificação de indivíduos.

Exemplo nº 18: Levantamentos estatísticos e combinação de informações dispersas

Para além da obrigação geral de respeitar as regras de proteção de dados, a fim de garantir o anonimato dos inquéritos estatísticos, os estatísticos estão sujeitos a um dever específico de sigilo profissional, sendo-lhes proibida, ao abrigo dessas regras, a publicação de dados não anónimos. Isto obriga-os a publicar dados estatísticos agregados que não podem ser atribuídos a uma pessoa identificada por detrás das estatísticas. Esta regra é particularmente relevante no que diz respeito à publicação de dados.

Em cada situação deverá ser determinado um limiar abaixo do qual se considere possível identificar as pessoas em causa. Se um critério parecer levar à identificação numa determinada categoria de pessoas, por maior que seja (ou seja, apenas um médico trabalha numa cidade de 6.000 habitantes), este critério "discriminatório" deveria ser totalmente abandonado ou outros critérios deveriam ser acrescentados para "diluir" os resultados sobre uma determinada pessoa, de modo a permitir o sigilo estatístico.

Exemplo nº 19: Publicação de videovigilância

Um lojista instala um sistema de vigilância por câmeras em sua loja. Ele publica, em sua loja, fotos de ladrões que foram flagrados pelo sistema de câmeras de vigilância. Após a intervenção policial, ele apaga os rostos dos ladrões, escurecendo-os. No entanto, mesmo após esta operação, ainda existe a possibilidade de as pessoas nas fotografias serem reconhecidas pelos seus amigos, familiares ou vizinhos, devido ao fato de, por exemplo, a sua figura, corte de cabelo e roupas ainda serem reconhecíveis.

4. QUARTO ELEMENTO: “PESSOA SINGULAR”

A proteção conferida pelas regras, aplica-se às pessoas singulares, ou seja, aos seres humanos. O direito à proteção dos dados pessoais é, nesse sentido, um direito universal que não se restringe aos nacionais ou residentes num determinado país.

Declaração Universal dos Direitos Humanos, segundo o qual “Toda pessoa tem direito ao reconhecimento, em qualquer lugar, como pessoa perante a lei”.

Dados Sobre Pessoas Mortas

As informações relativas a pessoas falecidas em princípio, não devem ser consideradas dados pessoais sujeitos às regras da LGPD, uma vez que os mortos já não são pessoas singulares no direito civil.

No entanto, os dados do falecido podem ainda receber indiretamente alguma proteção em certos casos. Por um lado, o responsável pelo tratamento dos dados pode não estar em condições de determinar se a pessoa a quem os dados se referem ainda está viva ou pode estar morta.

Dado que o responsável pelo tratamento dos dados está sujeito às obrigações de proteção de dados impostas pela lei no que diz respeito aos dados relativos a pessoas vivas, será provavelmente mais fácil para ele, na prática, tratar também os dados relativos aos mortos da forma imposta pelas regras de proteção de dados, em vez de separar os dois conjuntos de dados.

Por outro lado, as *informações sobre pessoas mortas também podem referir-se a pessoas vivas*. Por exemplo, a informação de que a falecida “Maria” sofria de hemofilia indica que o seu filho “Caio” também sofre da mesma doença, pois está ligada a um gene contido no cromossoma X. Assim, sempre que se possa considerar que as informações que constituem dados sobre os mortos dizem respeito, ao mesmo tempo, também aos vivos e são dados pessoais sujeitos à LGPD, os dados pessoais dos falecidos podem beneficiar indiretamente as regras de proteção de dados.

A obrigação de confidencialidade da equipe médica não termina com a morte do paciente. A legislação nacional sobre o direito à imagem e honra pode conceder também proteção à memória dos mortos.

- **Veja o que diz o JUSBRASIL:** No caso de familiares falecidos, os dados pessoais sensíveis podem incluir informações médicas, **genético hereditários**, financeiras, profissionais, entre outras. Esses dados devem ser protegidos, pois, mesmo após a morte do titular, ainda podem ter um impacto significativo na vida de familiares e outras pessoas envolvidas

Filhos não nascidos

Para determinar se as disposições nacionais em matéria de proteção de dados protegem também as informações sobre os nascituros, essa abordagem geral do sistema jurídico nacional deve ser considerada, juntamente com a ideia de que o objetivo das regras de proteção de dados é proteger o indivíduo.

Uma segunda questão é colocada pela consideração de que a resposta geral do sistema jurídico se baseia na expectativa de que a situação dos nascituros seja limitada no tempo ao período da gravidez. Não tem em conta o fato de esta situação pode durar consideravelmente mais tempo, como é o caso dos embriões congelados. Finalmente, podem ser encontradas respostas jurídicas específicas em disposições específicas sobre técnicas de reprodução, que tratam da utilização de informações médicas ou genéticas sobre embriões.

Pessoas jurídicas

Dado que a definição de dados pessoais se refere a pessoas singulares, ou seja, pessoas singulares, as informações relativas a pessoas jurídicas não são, em princípio, abrangidas pela lei e proteção por ela concedida não se aplica.

No entanto, certas regras de proteção de dados podem ainda aplicar-se indiretamente a informações relativas a empresas ou pessoas jurídicas, em diversas circunstâncias.

As informações sobre pessoas jurídicas também podem ser consideradas como “relativas” a pessoas singulares por mérito próprio, de acordo com os critérios estabelecidos. Este pode ser o caso quando o nome da pessoa jurídica deriva do nome de uma pessoa singular.

Outro caso pode ser o do e-mail corporativo, normalmente utilizado por determinado funcionário, ou o de informações sobre uma pequena empresa (juridicamente falando um “objeto” e não uma pessoa jurídica), que pode descrever o comportamento de seu proprietário.

Em todos estes casos, onde os critérios de “conteúdo”, “finalidade” ou “resultado” permitem a informação sobre a pessoa jurídica ou a empresa sejam consideradas “relativas” a uma pessoa singular, deverão ser consideradas dados pessoais e deverão aplicar-se as regras de proteção de dados.

4.1 O QUE ACONTECE SE OS DADOS FORA DA DEFINIÇÃO?

Em diferentes circunstâncias as informações podem ser consideradas como não sendo dados pessoais. Este é o caso quando os dados não podem ser considerados como relacionados com uma pessoa singular, ou porque a pessoa singular não pode ser considerada identificada ou identificável. Isto não significa, porém, que os indivíduos possam ser privados de qualquer tipo de proteção numa situação específica. *Se a LGPD não for aplicável, poderá aplicar-se a legislação nacional em matéria de proteção de dados.*

Como consideração geral, observou-se uma noção ampla de dados pessoais, mas esta noção não é ilimitada. Deverá ter-se sempre presente que o objetivo das regras contidas na LGPD é proteger os direitos e liberdades fundamentais dos indivíduos, em particular o seu direito à privacidade, no que diz respeito ao tratamento de dados pessoais. Estas regras foram, portanto, concebidas para serem

aplicadas a situações em que os direitos dos indivíduos possam estar em risco e, portanto, necessitarem de proteção e para pôr em vigor as disposições legislativas, regulamentares e administrativas necessárias para o seu cumprimento.

Pode, portanto, muito bem acontecer que certas situações que não envolvam o tratamento de dados pessoais, tal como definido na LGPD, sejam, no entanto, sujeitas a medidas de proteção ao abrigo da legislação nacional.

Outros conjuntos de regras, como a legislação sobre responsabilidade civil, o direito penal ou a legislação antidiscriminação, também podem proporcionar proteção aos indivíduos nos casos em que as regras de proteção de dados não se aplicam e em que vários interesses legítimos possam estar em jogo.

Os quatro principais “*blocos de construção*” que podem ser distinguidos na definição de “*dados pessoais*”: ou seja, “*qualquer informação*”, “*relativa a*”, “*uma pessoa identificada ou identificável*”, “*pessoa singular*”. Estes elementos estão intimamente interligados e alimentam-se uns dos outros, mas juntos determinam se uma informação deve ser considerada “*dado pessoal*”. A análise é apoiada por exemplos da prática nacional das APD europeias.

- **Qualquer informação:** exige uma interpretação ampla do conceito, independentemente da natureza ou conteúdo da informação e do formato técnico em que é apresentada. Isto significa que tanto a informação objetiva como a subjetiva sobre uma pessoa, seja qual for a sua qualidade, podem ser consideradas “*dados pessoais*”, independentemente do suporte técnico em que estejam contidas.
- **Relativo a:** tem sido até agora frequentemente ignorado, mas desempenha um papel crucial na determinação do âmbito substantivo do conceito, especialmente em relação a objetos e novas tecnologias. O parecer fornece três elementos alternativos, ou seja, conteúdo, finalidade ou resultado para determinar se a informação “*se relaciona com*” um indivíduo. Abrange também informações que possam ter um impacto claro na forma como um indivíduo é tratado ou avaliado
- **Identificado ou identificável:** centra-se nas condições sob as quais um indivíduo deve ser considerado como “*identificável*” e especialmente nos “*meios que possam ser razoavelmente utilizados*” pelo responsável pelo tratamento ou por qualquer outra pessoa para identificar esse indivíduo. O contexto e as circunstâncias particulares de um caso específico desempenham um papel importante nesta análise.
- **Pessoa física:** trata da exigência de que “*dados pessoais*” sejam sobre “*indivíduos vivos*”. O parecer discute também as interfaces com dados sobre pessoas falecidas, nascituros e pessoas coletivas. O parecer discute finalmente o que acontece se os dados ficarem fora do âmbito da definição de “*dados pessoais*”. Podem estar disponíveis diferentes soluções para lidar com questões nestes casos, incluindo legislação nacional.

Após centenas de horas de auditorias em empresas públicas e privadas, percebo um erro recorrente: muitas organizações acreditam que proteger dados pessoais significa apenas proteger CPF, RG e informações médicas. Essa visão simplificada impede uma análise adequada dos riscos previstos pela LGPD.

- Se uma simples imagem pode revelar identidade...
- Se um endereço IP pode identificar uma pessoa...
- Se um GPS pode monitorar comportamento...
- Então talvez ainda estejamos discutindo LGPD olhando apenas para CPF e RG.
- O verdadeiro desafio nunca foi identificar o dado.
- O verdadeiro desafio é compreender o contexto.

Estou em clientes onde até a Observação nos documentos são classificadas como dado pessoal e dado sensível.

Compreender essa diferença muda completamente a forma de estruturar programas de governança, realizar auditorias, elaborar RIPDs e tomar decisões sobre tratamento de dados.

10 conclusões que todo DPO deveria conhecer

1. Nem todo dado é dado pessoal.
2. Nem todo dado pessoal identifica alguém diretamente.
3. Anonimização não significa retirar o nome.
4. O contexto vale mais que o conteúdo.
5. Dados de pessoas jurídicas podem envolver pessoas naturais.
6. O conceito de identificabilidade evolui com a tecnologia.
7. A finalidade influencia a classificação.
8. O resultado do tratamento também importa.
9. A LGPD protege pessoas, não documentos.
10. O maior erro das organizações é classificar dados sem analisar seu contexto.

Fonte:

JUSBRASIL

01248/07/EN WP 136 GDPR - (Grupo de Trabalho do Artigo 29)

Wendel Babilon

babilon@wendelbabilon.com.br

Escritor, Auditor e Consultor Especializado em
Privacidade e Proteção de Dados

