

PROTEÇÃO LEGAL DE DADOS PESSOAIS E RESTOS MORTAIS



CICV

Comitè Internacional da Cruz Vermelha
19, avenue de la Paix
1202 Genebra, Suíça
T +41 22 734 60 01 F +41 22 733 20 57
shop@icrc.org www.icrc.org
© CICV, maio de 2017

PROTEÇÃO LEGAL DE DADOS PESSOAIS E RESTOS MORTAIS

ÍNDICE

1. INTRODUÇÃO	5
1.1 Introdução ao processo “Os Desaparecidos”	5
1.2 Proteção legal de dados pessoais e restos mortais	7
Objetivo do workshop eletrônico	7
O processo	7
2. PRINCÍPIOS COMUMENTE ACEITOS	9
2.1 Proteção de dados pessoais	9
a. Qualidade dos dados	9
b. Coleta e processamento de dados pessoais	11
c. Uso, divulgação e transferência de dados pessoais	18
d. Acesso às informações pessoais	21
2.2. Identificação de restos mortais	24
2.3 Proteção de informações genéticas	33



1. INTRODUÇÃO

1.1 Introdução ao processo “Os Desaparecidos”

A incerteza quanto à sorte dos familiares “desaparecidos” é uma dura realidade para inúmeras famílias, prolongada com frequência por muitos anos. Além de ser profundamente angustiante para as famílias, essa incerteza pode dificultar os esforços para obter a reconciliação e uma paz duradoura.

Para abordar a questão de pessoas desaparecidas e a situação de suas famílias o Comitê Internacional da Cruz Vermelha (CICV) lançou um processo de reflexão interativo.

Nesse sentido, estes foram os objetivos do CICV ao lançar esse processo, em cooperação com todos os envolvidos na abordagem da questão:

- revisar todos os métodos que poderiam ser utilizados de forma mais eficaz para evitar desaparecimentos e responder às necessidades das famílias que perderam contato com os entes queridos;
- definir recomendações comuns e complementares, assim como práticas operacionais, com todos os que trabalham na prevenção dos desaparecimentos, respondendo de modo apropriado quando pessoas são dadas como desaparecidas;
- posicionar essa preocupação entre as prioridades na agenda das autoridades governamentais, da Organização das Nações Unidas e de organizações não governamentais.

O processo foi conduzido em duas etapas.

Durante a primeira, diversos centros de pesquisa realizaram estudos paralelos à organização de workshops, que reuniram especialistas governamentais e não governamentais sobre temas relativos à questão das pessoas desaparecidas. Os estudos e workshops tiveram como finalidade ajudar a esclarecer as necessidades e os meios de satisfazê-las, além de definir as recomendações e as melhores práticas operacionais a serem implementadas. O presente workshop foi um desses eventos, listados abaixo:

- 2 workshops eletrônicos:
 - Restos mortais e ciência forense: workshop eletrônico preparatório;
 - Proteção legal de dados pessoais e restos mortais.
- 3 estudos:
 - Processo de luto e recordação;
 - Superação das tensões entre as necessidades familiares e os procedimentos judiciais;
 - Estudo sobre os mecanismos existentes para esclarecer a sorte das pessoas dadas como desaparecidas.
- 6 workshops realizados na seguinte ordem:
 - Membros das forças armadas / grupos armados: identificação, notícias familiares, mortos em combate, prevenção;
 - Restos mortais: legislação, política e ética;
 - Apoio às famílias das pessoas dadas como desaparecidas;
 - Restos mortais: gestão dos restos e das informações sobre os mortos;
 - Meios de prevenir desaparecimentos e tratar os casos de desaparecidos;
 - Mecanismos para solucionar questões sobre pessoas dadas como desaparecidas.

A fase preparatória de cada workshop compreendeu:

- A elaboração de documentos de referência baseados no Direito Internacional Humanitário (DIH) e no Direito Internacional dos Direitos Humanos (DIDH), assim como em lições ou experiências relevantes de situações de conflito armado ou violência do passado e do presente;
- Contribuições escritas de especialistas convidados a participar do workshop, tais como oficiais militares, altas autoridades governamentais, historiadores, advogados, acadêmicos e especialistas em medicina, psicologia e ciência forense.

Os documentos foram disponibilizados aos participantes através de uma *extranet* que lhes permitiu acompanhar todo o processo dos. Ao final de cada workshop, o CICV fez um resumo do resultado e enviou pela *extranet*. Opiniões individuais não foram registradas. A responsabilidade pelo resumo não coube nem aos participantes nem às organizações.

Além disso, o relatório final do workshop, incluindo o resultado, as contribuições dos especialistas e os documentos preparatórios do CICV, foi preparado e posteriormente publicado em inglês e francês.

Durante a segunda etapa, o CICV convocou uma conferência internacional de especialistas que participaram dos workshops e de partes interessadas. O evento foi realizado em Genebra de 19 a 21 de fevereiro de 2003.

Os resultados da primeira etapa foram distribuídos aos participantes da conferência na forma de um documento compilado pelo CICV, contendo todas as recomendações e melhores práticas, para a sua adoção pela conferência internacional em fevereiro de 2003. O documento levou em conta o resultado de todos os eventos.

O CICV espera que os resultados da conferência sejam úteis para:

- Indivíduos e organizações que trabalham nos âmbitos político, humanitário e de direitos humanos e sejam ativos no terreno; e
- Governos envolvidos no desenvolvimento do Direito Internacional e na prevenção ou resolução de conflitos, em especial no marco das Nações Unidas (por exemplo, através da Comissão de Direitos Humanos) ou do Movimento Internacional da Cruz Vermelha e do Crescente Vermelho (por exemplo, através da Conferência Internacional da Cruz Vermelha e do Crescente Vermelho).

1.2 Proteção legal de dados pessoais e restos mortais

Objetivo do workshop eletrônico

O objetivo do workshop foi definir princípios gerais básicos relativos à proteção legal de dados pessoais e à identificação de pessoas dadas como desaparecidas. Tais princípios poderiam ser respeitados no mundo inteiro a fim de assegurar as melhores práticas de todos os envolvidos na resolução de questões relativas às pessoas desaparecidas.

- É evidente que, em tais situações, continua sendo aplicável a legislação nacional, incluindo as normas de proteção de dados pessoais (caso existam).
- Em algumas situações, as normas nacionais podem simplesmente não existir ou não abordar uma questão específica (por exemplo, a coleta ou análise de amostras de DNA). Pode também não estar claro a quem se aplicam. Ou podem não ser aplicáveis na prática.
- Além disso, os órgãos governamentais podem não estar em condições de aplicar a lei, os serviços públicos talvez estejam desorganizados e diversas agências ou instituições internacionais e estrangeiras podem estar envolvidas.

Na prática, em diversos contextos não existe um marco legal apropriado, em termos de proteção da privacidade e dos dados pessoais, para a busca dos desaparecidos e a identificação dos restos mortais.

A finalidade do workshop foi, portanto, elaborar os princípios básicos a serem seguidos em qualquer situação e por todas as entidades envolvidas, evitando consequências prejudiciais e má gestão. Espera-se que esses princípios sejam aplicados por órgãos e agências locais, estrangeiros e internacionais, públicos e privados, independentemente do seu status e das imunidades ou privilégios especiais que possam ter à luz do Direito Internacional ou da legislação nacional. Limitam-se, porém, aos aspectos substantivos da proteção de dados pessoais e da identificação de pessoas dadas como desaparecidas. Não incluem os aspectos técnicos ou procedimentais do tratamento de dados, das análises de DNA ou da exumação.

O processo

O CICV elaborou um documento inicial contendo as propostas de redação dos princípios com base nos principais textos internacionais e em uma seleção de normas e regulamentos nacionais sobre o tema. O documento foi então enviado a uma equipe de juristas externos para duas rodadas de comentários através do workshop eletrônico. Os especialistas foram:

- Alejandra Gils Carbó, promotora e especialista em proteção de dados, Procuradoria-Geral, Argentina;
- Douwe Korff, consultor jurídico (direitos humanos e proteção de dados), Reino Unido;
- Eugene Oscanella, consultor jurídico (proteção de dados nas áreas da Medicina e da Genética), Canadá;
- Kosmas Tsiraktopoulos, Escritório do Comissário Federal de Proteção de Dados, Suíça.

O documento inicial foi reformulado duas vezes, de modo a levar em conta os comentários e sugestões feitos pelos juristas participantes.



2. PRINCÍPIOS COMUMENTE ACEITOS

2.1 Proteção de dados pessoais

a. Qualidade dos dados

PRINCÍPIO 1

O termo “dados pessoais” se refere a quaisquer informações relacionadas a um indivíduo identificado ou identificável.

Na maioria dos textos nacionais e internacionais, a definição de “dados pessoais” é muito ampla. A *Convenção do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais* (1981) (Convenção do CdE) define “dados pessoais” como “qualquer informação relativa a um indivíduo identificado ou identificável”. Essa definição é ampla o suficiente para incluir todos os dados biométricos, incluindo informações médicas e genéticas.

Uma pessoa “identificável” é uma pessoa que pode ser identificada direta ou indiretamente. Isto não significa que os dados tenham de ser vinculados a uma pessoa cujo nome é conhecido: informações sobre pessoas vivas cujo nome é desconhecido (como as impressões digitais de um suspeito que se recusa a dar o nome em uma delegacia ou os dados médicos sobre uma vítima de acidente internada no hospital ainda sem nome) também são “pessoais”. A definição é mais complexa quando se trata de dados semi-identificáveis, tais como informações sob pseudônimo ou que poderiam ser ligadas a um indivíduo identificado por certas pessoas em determinadas circunstâncias, mas não por outras em circunstâncias distintas. Algumas legislações consideram que tais dados são sempre pessoais e sujeitos a normas de proteção (mesmo que tratados por alguém sem acesso à “chave” de identificação), embora a aplicação das normas possa ser menos rigorosa. Outras consideram que tais dados são pessoais somente com relação a alguém que tenha acesso à “chave”, mas sustentam que outras normas gerais sobre o tratamento de dados codificados possa ser aplicável; há outras, ainda, que isentam completamente esses dados de quaisquer restrições jurídicas.

Dados mais qualitativos, tais como estilos de vida, atividades, participação em determinados eventos, associações, etc., incluem-se no termo “dados pessoais” desde que sejam relativos a um indivíduo identificado ou identificável. Por exemplo, a *Lei de Informação* russa define dados pessoais como “relatórios sobre fatos, eventos, estilos de vida de cidadãos que permitem a identificação de indivíduos”.¹ Outras legislações nacionais têm definições igualmente amplas. A coleta, a utilização e a divulgação desse tipo de dados estão, portanto, sujeitas aos mesmos princípios que os de quaisquer outros dados pessoais. Também estão sujeitas às garantias específicas para a coleta e o tratamento de dados sensíveis, caso tais informações forem assim consideradas ou se puderem levar à divulgação de outros dados individuais sensíveis.

Algumas legislações nacionais aplicam-se apenas à proteção dos dados pessoais de um indivíduo vivo (por exemplo, a *Lei de Proteção de Dados* do Reino Unido). Portanto, as informações relativas a pessoas falecidas não estão sujeitas às normas de proteção de dados. Outras legislações estabelecem normas específicas em determinadas circunstâncias. A *Lei de Registros Pessoais* da França permite o tratamento de dados sobre mortos para fins de pesquisas médicas, a menos que, em vida, a pessoa tenha se oposto expressamente. Há ainda outras legislações que estipulam que os dados pessoais sobre indivíduos que morreram há um tempo determinado não serão mais considerados como tais para determinados fins. De acordo com a *Lei de Privacidade* canadense, que regula as práticas de tratamento de dados das instituições federais, as informações sobre uma pessoa morta há mais de 20 anos não são consideradas “informações pessoais” na aplicação de certas seções da lei. Desse modo, por exemplo, as normas da Lei que impedem o uso de dados pessoais para fins incompatíveis com o objetivo da sua coleta original, assim como aquelas que limitam a divulgação de tais dados, não se aplicam a tais informações. Isto pode ter implicações para o uso e divulgação de informações sobre indivíduos dos quais se sabe que estão mortos, mas cujos restos mortais não foram localizados. Uma ordem ou declaração judicial reconhecendo uma morte presumida permitiria que as informações sobre a pessoa fossem usadas para ajudar a localizar essa pessoa ou os restos mortais. Os procedimentos e o período de tempo necessários para que se presuma a morte de uma pessoa variam conforme cada província canadense.

“Dados sensíveis”

A maioria das legislações nacionais inclui uma categoria de dados considerados sensíveis e que estão sujeitos a garantias específicas. Não há uma definição padrão para “dados sensíveis”. Essa categoria normalmente não é definida com precisão, mas aparece como uma lista de tipos de dados sujeitos à proteção específica ou como características pessoais que não podem ser motivo de discriminação.

Dados sobre origem étnica ou racial, opiniões políticas, crenças religiosas, filosóficas ou de outra natureza, saúde, vida sexual, condenações penais e filiação a sindicato ou associação estão incluídos na maioria dos textos nacionais ou internacionais como dados sensíveis. A *Lei de Proteção sobre Dados Pessoais* do Chile, por exemplo, define dados sensíveis como dados pessoais relativos a características físicas ou morais de pessoas ou a fatos ou circunstâncias da sua vida íntima ou privada, tais como hábitos pessoais, origem racial, ideologias, opiniões políticas, crenças ou convicções religiosas, condições de saúde física ou psicológica e vida sexual. Em outras legislações, os dados sensíveis aparecem como uma lista fechada.

Embora esses tipos de dados pessoais sejam quase sempre considerados sensíveis, outros tipos também podem entrar nessa categoria. Praticamente

1 Tradução livre do CICV.

qualquer informação pessoal pode ser considerada sensível em determinadas circunstâncias. Em vez de limitar os dados sensíveis a uma lista de dados que não podem ser motivo de discriminação, eles poderiam ser definidos como informações pessoais que podem ser usadas em detrimento do titular (ou seja, o indivíduo a quem os dados se referem). Dados sensíveis também são aqueles a partir dos quais se podem inferir informações pessoais sensíveis ou que podem levar à divulgação de tais informações.

A maioria dos dados coletados com o objetivo de estabelecer a identidade, o paradeiro ou a sorte de pessoas desaparecidas entrariam na categoria de dados sensíveis.

“Dados médicos” (ou “informações sobre saúde”)

O termo “dados médicos” refere-se a todos os dados pessoais relativos à saúde de um indivíduo. Também diz respeito às informações que têm uma ligação clara e estreita com a saúde, incluindo os dados genéticos. A *Lei de Proteção de Informações Pessoais e Documentos Eletrônicos* do Canadá, que se aplica a empresas comerciais operando sob jurisdição federal, define “informações pessoais de saúde” como “relativas a um indivíduo, vivo ou falecido [...]”.

- informações sobre a saúde física ou mental do indivíduo;
- informações sobre qualquer serviço de saúde prestado ao indivíduo;
- informações sobre a doação, pelo indivíduo, de qualquer parte do corpo ou qualquer substância corporal, assim como quaisquer informações obtidas a partir de testes ou exames de uma parte do corpo ou substância corporal;
- informações obtidas no decurso da prestação de serviços de saúde ao indivíduo; ou
- informações obtidas incidentalmente para a prestação de serviços de saúde ao indivíduo.”²

As informações de saúde são consideradas dados sensíveis na maioria dos textos nacionais e internacionais, estando sujeitas a normas de divulgação específicas. Existe também uma tendência a considerar as informações de DNA como dados sensíveis, ou como uma categoria especial de dados sujeitos a normas mais rigorosas de proteção, embora isto geralmente não esteja especificamente previsto nos textos jurídicos.

b. Coleta e processamento de dados pessoais

Normas nacionais e internacionais sobre a proteção de dados pessoais têm sido adotadas para proteger os indivíduos contra as invasões do seu direito à privacidade por parte de autoridades do Estado ou organismos privados. No contexto da busca por pessoas desaparecidas, os dados são coletados, processados e divulgados principalmente em benefício do titular, não no interesse de terceiros ou no interesse público.

PRINCÍPIO 2

Os dados pessoais devem ser coletados e tratados de maneira justa e legal.

Esse é um princípio reconhecido tanto em textos internacionais, como as *Diretrizes das Nações Unidas para a Regulação de Arquivos de Dados Pessoais Informatizados* de 1990 (*Diretrizes da ONU*), a *Convenção do Conselho da Europa (CdE)* e as *Diretrizes da Organização para a Cooperação e o Desenvolvimento Econômico para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais* de 1980 (*Diretrizes da OCDE*), como em textos nacionais (Argentina, Canadá, Chile, França e Suíça).

2 Tradução livre do CICV.

O termo “tratamento” geralmente inclui qualquer operação ou conjunto de operações realizadas sobre dados pessoais. A *Diretriz 95/46/EC do Parlamento Europeu e do Conselho de 24 de outubro de 1995 sobre a Proteção de Indivíduos relativa ao Tratamento de Dados Pessoais e à Livre Circulação desses Dados* (Diretriz 95/46/EC) define “tratamento” como “qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como coleta, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocar à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição” (ver também a *Lei de Proteção de Dados de 1998 do Reino Unido* e a *Lei de Proteção de Dados Pessoais da Argentina*).

O fato de um método de coleta ser justo depende, em parte, do tipo de dados a serem coletados e do seu uso (por exemplo, dados utilizados para fins de aplicação da lei vs. dados coletados para receber benefícios de bem-estar social). O método não deverá ser enganoso, fraudulento ou contrário à lei. Esse princípio tem como objetivo assegurar que os indivíduos não sejam induzidos ao erro ou ludibriados quanto à finalidade pela qual os dados são coletados. Também implica que o consentimento com relação à coleta não deve ser obtido por meio de engano.

Quando os dados não forem obtidos diretamente do titular, o responsável pelo controle de dados – isto é, a pessoa, autoridade, agência ou outro órgão que determina a finalidade e a maneira pelas quais os dados são tratados – nem sempre estará em condições de atestar ou verificar se as informações foram obtidas mediante métodos justos e legais por intermediários que não são os representantes do titular. Isto deve ser aceito como uma dificuldade persistente ao se tentar localizar pessoas desaparecidas. O problema é semelhante ao enfrentado pelos policiais ao conduzirem investigações. Eles próprios podem estar sujeitos a normas que exigem a justa obtenção de informações para os seus inquéritos (normas sobre vigilância eletrônica, por exemplo), mas, se obtém informações de outra fonte, não estão obrigados a ignorá-las. A mesma lógica pode se aplicar no caso das pessoas desaparecidas. Como o objetivo primordial e válido é localizar tais indivíduos, um responsável que coleta informações que podem ter sido obtidas indevidamente por outros deve, contudo, ser autorizado a recolher essas informações, desde que não esteja implicado de forma alguma nessa coleta inadequada e não a tenha incentivado ou tolerado. No entanto, ele deve estar particularmente alerta para o fato de que as informações podem ser imprecisas.

PRINCÍPIO 3

O consentimento do indivíduo é necessário para a coleta e a utilização de dados pessoais, salvo quando for inapropriado.

A maioria dos textos nacionais e internacionais estabelece que o consentimento do indivíduo deve geralmente ser obtido antes da coleta dos dados. Alguns parecem não exigir o consentimento, mas preveem o direito de se opor ao tratamento dos dados pessoais (França). Algumas leis especificamente permitem que o consentimento seja retirado, sujeito a restrições legais e comunicação razoável (Argentina e Canadá).

Legislações nacionais (Canadá, Argentina e Suíça) determinam que o consentimento deve ser livre e informado. Por exemplo, a *Lei de Proteção de Informações Pessoais e Documentos Eletrônicos* do Canadá afirma que o princípio requer “conhecimento e consentimento”, isto é, deve-se realizar um esforço razoável para assegurar que o indivíduo seja avisado sobre os objetivos para os quais as informações serão utilizadas, e os objetivos devem ser indicados

de modo que o indivíduo possa entender como os dados serão usados ou comunicados. A *Lei de Proteção de Dados Pessoais* da Argentina estabelece que as seguintes informações devem ser fornecidas para a pessoa à qual os dados coletados se referem:

- a finalidade para a qual as informações foram coletadas e a quem se destinam, incluindo sua transferência a terceiros;
- a existência de arquivos, registros e bases de dados que usam informações pessoais;
- o caráter obrigatório ou facultativo da informação requisitada;
- as possíveis consequências de não fornecer os dados ou de oferecer dados imprecisos;
- a possibilidade de o indivíduo exercer o direito de acesso aos dados pessoais, de retificá-los ou de suprimi-los.

Podem-se encontrar deveres de informação similares em outras legislações (por exemplo, a da França).

A forma em que se procura obter o consentimento pode variar dependendo das circunstâncias e do tipo de informação coletada. O consentimento implícito pode ser considerado razoável em alguns casos, por exemplo quando a pessoa fornece as informações por vontade própria para um fim específico.

As expectativas razoáveis de um indivíduo também podem ser levadas em conta. As circunstâncias em que os dados podem ser coletados sem o consentimento ou conhecimento da pessoa são geralmente estipuladas em determinadas disposições jurídicas e estão sujeitas a requisitos específicos. Tais circunstâncias normalmente se relacionam com a proteção de um interesse público (manutenção da ordem pública e investigações criminais, comunicação de dados entre agências governamentais e proteção da saúde pública) ou com casos em que a coleta de informações é claramente do interesse do indivíduo em questão e quando o consentimento não pode ser oportunamente obtido (Argentina, Canadá e Alemanha).

Um funcionário do CICV preenche o formulário de solicitação de busca para a mãe de uma pessoa desaparecida.



Dada a natureza das informações relativas às pessoas desaparecidas, obter o consentimento dos indivíduos sobre os quais os dados são coletados e tratados pode ser inadequado ou impossível. A coleta de dados pessoais com o objetivo de localizar um desaparecido pode, no entanto, ser considerada como claramente do interesse de tal pessoa. Portanto, as informações pessoais a serem usadas com essa finalidade poderiam ser coletadas sem o consentimento ou conhecimento do indivíduo.

Em circunstâncias nas quais os dados são coletados sem consentimento, porém, o indivíduo conserva o direito de ser informado sobre a existência, a utilização e a divulgação das suas informações pessoais. A *Recomendação (87) 15* do Comitê de Ministros do Conselho da Europa que regulamenta a utilização de dados pessoais no setor da polícia, por exemplo, afirma que, a menos que os dados forem destruídos, o indivíduo deve ser informado, sempre que possível, de que são mantidas informações sobre ele tão logo o objetivo das atividades policiais não possa mais ser prejudicado (§ 2.2).

Caso as informações pessoais sejam obtidas de outro indivíduo ou de terceiros sem o consentimento ou conhecimento do titular, este deve ser informado, logo que possível, da existência de informações pessoais sobre si. O princípio de consentimento implica que uma pessoa tem o direito de se opor ao tratamento dos dados pessoais que lhe dizem respeito ao ser informada da coleta e do tratamento. Tais informações devem então ser excluídas de um tratamento posterior se não houver nenhum interesse primordial contra essa interrupção.

PRINCÍPIO 4

A coleta e o tratamento de dados pessoais devem se limitar ao que for necessário para a finalidade identificada no momento ou antes da coleta.

Um princípio básico da coleta de dados pessoais é que esta não pode ser feita indiscriminadamente, com um objetivo indeterminado ou a ser determinado somente no futuro. O princípio da especificação da finalidade é reconhecido em textos internacionais (Diretrizes da ONU, Convenção do CdE e Diretrizes da OCDE) e nacionais (Argentina, Canadá e Reino Unido).

A finalidade da coleta de dados deve ser legal e apropriada. Deve existir uma conexão razoável entre a missão ou as atividades da organização e o propósito da coleta. A *Lei de Privacidade* do Canadá afirma que “nenhuma informação pessoal deve ser coletada por uma instituição governamental, a menos que se relacione diretamente com um programa operacional ou atividade da instituição”.³ De modo similar, a *Lei de Proteção de Informações Pessoais* do Canadá estabelece que “uma organização só pode coletar, utilizar ou divulgar informações pessoais para fins que uma pessoa razoável consideraria apropriados em tais circunstâncias”.⁴

O princípio da especificação da finalidade também significa que o volume e o tipo de informações coletadas e armazenadas devem se limitar ao que for necessário para cumprir o objetivo especificado. A coleta e o armazenamento não devem ser excessivos em relação ao propósito pelos quais os dados são tratados. Do mesmo modo, o uso de informações pessoais coletadas deve se limitar ao cumprimento do objetivo determinado. Os dados pessoais não podem ser usados para outras finalidades ou para fins incompatíveis com o objetivo pelo qual os dados foram obtidos e tratados.

³ Tradução livre do CICV.

⁴ Idem.

Em conformidade com o princípio do consentimento informado, o objetivo deve ser comunicado ao titular. Também deverá ser divulgado a qualquer terceiro que forneça dados sobre tal pessoa, já que o terceiro deve ser capaz de determinar se a utilização e a transferência das informações são consistentes com os princípios de proteção de informações. Se os dados pessoais forem obtidos de uma pessoa que não seja o titular, essa pessoa deve ser informada: a) sobre a finalidade da coleta; b) se a resposta é voluntária ou exigida por lei; c) sobre as possíveis consequências de se negar a responder; e d) que o titular tem direitos de acesso e proteção dos dados pessoais.

O princípio é aplicável, *a priori*, à coleta, à utilização e ao armazenamento de todos os dados pessoais. Qualquer exceção a esse princípio deve ser claramente mencionada na lei. O artigo 9.º da Convenção do CdE permite a derrogação desse princípio caso seja “uma medida necessária em uma sociedade democrática no interesse da [...] proteção da segurança do Estado, da segurança pública, [...] ou da repressão de delitos penais; [ou] proteção dos dados da pessoa em questão ou dos direitos e liberdades de outros”. De acordo com esse princípio, a *Recomendação* do Conselho de Ministros reafirma, por exemplo, que a coleta de dados pessoais para fins policiais deve-se limitar ao que for necessário para a prevenção de um perigo real ou a repressão de um determinado delito penal.

No contexto da busca de pessoas desaparecidas, é especialmente importante o respeito pelo objetivo predeterminado para o qual os dados pessoais foram coletados e tratados, uma vez que muitas exceções às normas gerais de proteção de dados podem ser invocadas alegando-se que são do interesse vital do desaparecido. Os principais objetivos da coleta de dados com relação a pessoas dadas como desaparecidas são:

- estabelecer a identidade, localização, condições e sorte de pessoas vivas que estão desaparecidas;
- estabelecer a identidade, localização, condições e sorte de pessoas falecidas que estão desaparecidas;
- dar às famílias informações sobre o paradeiro, condições e sorte dos entes queridos desaparecidos.

Para esses propósitos, os dados coletados podem incluir:

- para pessoas vivas que estão desaparecidas:
 - dados administrativos (nome, lugar de residência, etc);
 - dados qualitativos (detalhes sobre a profissão, atividades, último paradeiro conhecido, etc.);
 - dados biométricos (sexo, idade, descrição, etc); os dados de DNA geralmente não são coletados para pessoas vivas que estão desaparecidas;
- para pessoas falecidas e não identificadas:
 - dados administrativos (nome, lugar de residência, etc);
 - dados qualitativos (detalhes sobre a profissão, atividades, último paradeiro conhecido, etc.);
 - dados biométricos (sexo, idade, descrição, etc), incluindo os dados de DNA;
- para familiares:
 - dados administrativos (nome, lugar de residência);
 - dados de DNA.

Entre as fontes, incluem-se o indivíduo desaparecido (por exemplo, dados *ante mortem* ou *post mortem*), familiares, testemunhas e organismos públicos ou privados (agências governamentais, organizações internacionais e não governamentais). As técnicas e os procedimentos usados para a busca dos desaparecidos e a identificação dos restos mortais variam consideravelmente

dependendo do contexto, do período de tempo, da escala dos acontecimentos e da situação política. A extensão e o tipo de dados coletados podem variar da mesma forma.

As atividades realizadas após a coleta de dados podem incluir:

- comparação das informações de diferentes fontes, o que pode envolver:
 - comparação das informações coletadas de diferentes fontes públicas e privadas;
 - divulgação pública das informações coletadas;
 - análise e cruzamento dos dados de DNA;
- fornecimento de informações sobre os resultados do tratamento, como por exemplo:
 - pessoas vivas que estão desaparecidas (quando encontradas);
 - familiares;
 - autoridades públicas;
 - organizações privadas.

A aplicação do princípio da especificação da finalidade implica a limitação da coleta e do tratamento dos dados obtidos para outros fins que não sejam o de estabelecer a identidade, o paradeiro e a sorte de um desaparecido, mas que poderiam ser usados com esse objetivo. Os dados coletados para outros fins que não sejam o da identificação podem ser tratados somente na medida em que forem utilizados exclusivamente para buscar e identificar pessoas desaparecidas (um interesse vital do desaparecido). Além disso, somente os dados necessários para esse efeito devem ser transferidos por um terceiro que mantém esses dados (ver *Princípio 8* abaixo). Um terceiro que armazena dados pessoais coletados com outro objetivo é responsável pelo uso das informações que transfere ou divulga. Na obtenção de dados sobre pessoas naturais, vivas ou falecidas, de fontes públicas ou privadas, deve-se portanto procurar garantir que as informações serão divulgadas somente se:

- foram coletadas para estabelecer a identidade, o paradeiro ou a sorte de pessoas desaparecidas;
- a divulgação não é incompatível com o objetivo para o qual os dados foram coletados ou obtidos;
- os dados originam-se de fontes acessíveis ao público (como registros públicos ou profissionais ou diretórios publicados);
- a divulgação atende a um interesse vital da pessoa a quem os dados se referem ou de um familiar próximo, quando tal pessoa esteja física ou legalmente impossibilitada de dar o consentimento para a divulgação.

PRINCÍPIO 5

Os dados sensíveis só devem ser coletados e tratados com as garantias adequadas.

Textos nacionais e internacionais estabelecem restrições específicas sobre o tratamento de dados sensíveis. São necessárias salvaguardas para evitar a discriminação ilegal e o uso de informações pessoais que poderiam prejudicar o titular. Podem-se encontrar diferentes mecanismos de salvaguarda na legislação nacional, seja em normas sobre proteção geral de dados ou em leis específicas (por exemplo, proteção de registros médicos, perfis de DNA ou fichas criminais). De acordo com a *Lei de Proteção de Dados* da Suíça, deve-se registrar a coleta de dados sensíveis junto ao Comissário Federal de Proteção de Dados do país. A *Lei sobre Registros Pessoais* da França exige o expresso consentimento do indivíduo. A *Lei de Proteção de Dados Pessoais* da Argentina estabelece que ninguém será obrigado a fornecer dados pessoais sensíveis, que só podem ser coletados “em circunstâncias de interesse geral autorizadas por lei”.

Dados sensíveis são definidos nas *Diretrizes das Nações Unidas* como informações suscetíveis de dar origem a discriminação ilegal ou arbitrária. As *Diretrizes* estabelecem que tais dados não devem ser compilados. No entanto, permitem-se exceções dentro dos limites dispostos pelos instrumentos internacionais de direitos humanos, isto é, aqueles que definem discriminação ilegal ou arbitrária. Também poderia haver exceções no âmbito da “cláusula de exceção humanitária”, que estabelece que “pode ser expressamente prevista uma derrogação dos presentes princípios quando um arquivo tiver por objetivo a proteção dos direitos humanos e liberdades fundamentais do indivíduo ou a prestação de assistência humanitária”. Por conseguinte, pode-se permitir, segundo as *Diretrizes*, a coleta de dados sensíveis por motivos humanitários.

O artigo 6.º da *Convenção* do CdE afirma que se devem adotar garantias adequadas para dados sensíveis, mas a *Convenção* não especifica o que seriam “garantias adequadas”. A *Recomendação* do Conselho de Ministros, que regula o uso de dados pessoais no setor policial estabelece que “deve ser proibida a coleta de dados sobre indivíduos somente com base exclusivamente na sua determinada origem racial, determinadas convicções religiosas, comportamento sexual ou opiniões políticas, ou porque pertencem a certos movimentos ou organizações que não são proibidos por lei”.⁵ A coleta de dados relativos a esses fatores só pode ser realizada se isso for “absolutamente necessário para o objetivo de uma determinada investigação”(2.4).⁶ De modo similar, a *Diretriz 95/46/EC* proíbe o tratamento de dados sensíveis, mas prevê derrogações, inclusive quando o tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento”.⁷

No contexto da busca pelas pessoas desaparecidas e da identificação dos restos mortais, dados sensíveis como origem étnica, atividades religiosas ou políticas, associações, etc., podem ser necessários para determinar a sorte e o paradeiro dos desaparecidos ou a identidade dos restos mortais.

Na medida em que tal coleta seja por motivos humanitários ou para o benefício do titular, a obtenção e o tratamento de informações sensíveis devem ser permitidos. Deve-se ter especial cuidado em assegurar que os dados não sejam usados ou divulgados em circunstâncias que seriam prejudiciais ao indivíduo em questão.

PRINCÍPIO 6

Os dados pessoais devem ser precisos, completos e atualizados conforme o necessário para a finalidade para a qual são usados.

As informações serão mais ou menos precisas, completas e atualizadas dependendo da sua utilização. Os dados devem ser suficientemente precisos, completos e atualizados para minimizar a possibilidade de que uma decisão prejudicial a uma pessoa seja tomada com base em informações inadequadas.

Esse princípio não exclui a coleta de informações incompletas ou duvidosas. Os dados que não puderem ser totalmente verificados podem ser considerados como precisos e atualizados desde que as dúvidas ou incertezas acerca da exatidão e a atualização sejam registradas com os dados. Se forem divulgadas a terceiros, tais informações devem ser acompanhadas da respectiva declaração ou nota qualificativa.

⁵ Tradução livre do CICV.

⁶ Idem.

⁷ Idem.



Depois que uma família realiza a solicitação de busca, o CICV a visita para coletar informações detalhadas sobre a pessoa desaparecida. As informações incluem dados como as características físicas da pessoa desaparecida e as circunstâncias do seu desaparecimento.

PRINCÍPIO 7

Os dados pessoais devem ser protegidos por garantias de segurança adequadas à sensibilidade das informações.

Devem-se estabelecer garantias de segurança para proteger os dados pessoais contra perda ou roubo, acesso não autorizado, divulgação, cópia, uso ou modificação, independentemente do formato em que foram armazenados. As salvaguardas podem incluir tanto a segurança física (por exemplo, restrição do acesso aos estabelecimentos que guardam os registros) como medidas de segurança técnica (criptografia, *firewalls*, entre outras). As pessoas e os funcionários que manipularem ou tratarem os dados devem assinar um termo de confidencialidade.

A natureza das garantias pode variar dependendo da sensibilidade das informações. Dados mais sensíveis devem receber um nível maior de proteção (ver, por exemplo, o *Código Modelo para a Proteção de Informações Pessoais* da Associação de Padrões Canadenses).

c. Uso, divulgação e transferência de dados pessoais

PRINCÍPIO 8

Os dados pessoais não podem ser usados, divulgados ou transferidos com fins diferentes daqueles para os quais foram coletados sem o consentimento da pessoa em questão, salvo se exigido por um interesse público considerável ou para a proteção de interesses vitais de tal pessoa ou de outras.

O direito à privacidade exige que as informações pessoais sejam protegidas contra a divulgação. Tais informações só podem ser difundidas com a finalidade para a qual foram obtidas ou compiladas, ou para uma utilização compatível com esse fim.

A legislação nacional pode estabelecer que, sem autorização, as informações só podem ser utilizadas com a finalidade para a qual foram obtidas ou para usos compatíveis com tal objetivo. No entanto, em certas circunstâncias os dados pessoais podem ser utilizados ou divulgados sem o consentimento ou conhecimento do indivíduo. Informações pessoais de terceiros (familiar, testemunhas e outras vítimas) podem também ter de ser divulgadas para a busca de um desaparecido. As exceções, bastante amplas, normalmente incluem circunstâncias específicas:

- quando a divulgação é necessária para fins de aplicação da lei, para a realização de uma investigação ou em procedimentos judiciais;
- quando a divulgação é necessária para evitar ou minimizar uma ameaça grave ou imediata à saúde ou segurança do indivíduo ou de outros;
- quando a divulgação claramente beneficiará o titular; ou
- quando a divulgação é para fins estatísticos ou de pesquisa.

A *Lei Federal de Proteção de Dados* da Alemanha permite o uso de dados coletados com outro objetivo se a lei o exigir, se o titular der consentimento, se ficar evidente que será do interesse da pessoa em questão e não houver razão para presumir que ela retiraria o seu consentimento se soubesse da outra finalidade, ou ainda se isto for necessário para evitar uma grave violação dos direitos de outra pessoa. De acordo com a *Lei de Privacidade* do Canadá, as informações pessoais mantidas por autoridades públicas podem ser divulgadas, entre outros motivos, “se o interesse público na divulgação claramente prevalecer sobre qualquer invasão de privacidade que possa decorrer da divulgação” ou se “a divulgação claramente beneficiar o titular”.⁸

Os dados pessoais só devem ser divulgados a terceiros com o consentimento do titular e para as finalidades acima mencionadas com relação à busca e identificação de pessoas desaparecidas. Quando isto não for óbvio nas circunstâncias, ou se o consentimento não puder ser obtido de maneira prática, os dados devem ser fornecidos com a condição de que somente sejam usados para os fins estabelecidos. Em determinadas circunstâncias, os dados pessoais coletados com o objetivo de estabelecer a identidade, a localização e a sorte de pessoas desaparecidas podem ser fornecidos para servir a outros interesses do desaparecido ou dos seus familiares, ou a um interesse público, especialmente em conexão com investigações criminais ou procedimentos jurídicos. No entanto, também devem-se considerar os legítimos interesses compensatórios do indivíduo ou de outras pessoas (por exemplo, se houver uma ameaça à segurança da pessoa).

A divulgação pública de dados pessoais (colocá-los à disposição da imprensa ou da população) sem o consentimento do titular só deve ser considerada se manifestamente vier a servir para proteger ou assegurar os interesses vitais dessa pessoa ou de outra e quando o consentimento não puder ser obtido de maneira legal ou prática. Contudo, devem-se considerar também os legítimos interesses compensatórios ou de outras pessoas contra a publicidade ou publicação.

A coleta, o tratamento ou a divulgação ilegais de dados pessoais podem dar origem à responsabilidade civil se o titular sofrer danos. Em situações de conflito armado ou violência interna generalizada, é provável que o respeito pelos princípios de proteção de dados receba pouca prioridade por parte dos envolvidos no conflito. A ameaça de responsabilidade civil por infrações das normas de proteção de dados possivelmente tenha pouco impacto durante as hostilidades. Após o conflito, no entanto, a responsabilidade civil poderia ser imposta em virtude das infrações. Uma pessoa poderia obter compensação se a indevida coleta, utilização ou divulgação de dados pessoais lhe ocasionar danos.

8 Tradução livre do CICV.

PRINCÍPIO 9

As informações pessoais só podem ser transferidas a terceiros respeitando-se os princípios de proteção de dados.

Como a proteção de informações pessoais proporcionada pela legislação nacional é geograficamente limitada, diversos Estados adotaram normas sobre a transferência de dados pessoais, submetendo-a a um controle prévio, autorização ou declaração. A lei suíça proíbe a transmissão desse tipo de dados ao exterior se isso constituir uma grave ameaça (embora não física) às pessoas interessadas, em particular se o nível de proteção dessas informações não for equivalente aos previstos pela lei suíça. A transmissão de dados sensíveis pode estar sujeita a condições mais rigorosas. A lei suíça estabelece que “ninguém tem o direito de transmitir dados sensíveis ou perfis de personalidade a terceiros sem justificativa”.⁹ A Diretriz 95/46/EC, de modo similar, restringe a transferência de dados pessoais a terceiros países com um nível de proteção adequado.

O responsável pelos dados deve assegurar, quando for possível e apropriado, que as outras pessoas ou órgãos envolvidos na coleta dos dados tenham agido e continuarão agindo de acordo com todas as leis e regulamentos de proteção de dados relevantes e aplicáveis, na medida em que essas leis e regulamentos sejam compatíveis com o Direito Internacional dos Direitos Humanos, o Direito Internacional Humanitário e as normas e padrões de proteção de dados. O responsável deve também procurar garantias de que, se transferir informações pessoais a um terceiro, este respeitará os princípios, normas e regulamentos de proteção de dados.

PRINCÍPIO 10

Devem-se eliminar os dados pessoais logo que o objetivo da sua coleta for alcançado ou quando não forem mais necessários. As informações podem, no entanto, ser retidas por um período definido caso isso seja necessário para o benefício do titular ou se for essencial para o desempenho das tarefas humanitárias da organização que as coletou.

As informações pessoais só devem ser retidas enquanto isso for necessário para a realização do objetivo especificado no momento da coleta. Esse princípio vincula-se estreitamente com o da especificação da finalidade. Os dados pessoais que já não forem necessários para alcançar tal objetivo devem ser eliminados, apagados ou armazenados de forma que não se possa mais identificar a pessoa que os forneceu. Se tais dados tiverem de ser usados para um novo propósito, deve-se buscar o consentimento do indivíduo.

Em determinadas circunstâncias, os dados pessoais podem ser armazenados ou retidos. Por exemplo, informações pessoais que foram usadas para tomar uma decisão sobre um indivíduo devem ser retidas durante um tempo suficiente para permitir que essa pessoa tenha acesso a elas após a decisão. De modo similar, as informações podem ser úteis para o titular durante processos civis ou penais. No entanto, os dados não devem ser mantidos indefinidamente após o fim do prazo pré-determinado. Considerando o mandato e as atividades de algumas organizações humanitárias, porém, os arquivos dos dados podem ser mantidos por um longo período após o término das relações entre o indivíduo e a organização. Portanto, deve-se permitir um período maior de retenção por motivos humanitários.

9 Tradução livre do CICV.

d. Acesso às informações pessoais

PRINCÍPIO 11

O titular deve ter acesso aos dados pessoais. Deve-se igualmente prever o direito de contestar a exatidão e a integralidade das informações, modificando-as se for o caso.

Textos nacionais e internacionais preveem o direito de acesso para a pessoa à qual as informações se referem. Devem-se estabelecer procedimentos adequados para esse efeito. Os princípios gerais sobre o acesso consagrados nos respectivos instrumentos internacionais e legislações nacionais são os seguintes:

- todas as pessoas devem ser informadas da existência, uso e divulgação dos dados pessoais que a elas se referem;
- mediante pedido, uma pessoa tem direito de acesso a tais informações e de obter uma cópia;
- todas as pessoas têm direito de contestar a exatidão e a integridade das informações pessoais que a elas se referem e de modificá-las conforme o caso, ou pelo menos de inserir uma anotação no seu arquivo indicando o seu desejo de que a informação seja corrigida;
- devem-se prever medidas caso tais direitos sejam negados.

No entanto, em determinadas situações, uma organização ou autoridade pública pode não ser autorizada por lei a prover acesso a todas as informações que mantém sobre um indivíduo. Em outros casos, a organização ou a autoridade pode ter o poder de recusar ou divulgar dados ao seu critério. Além disso, as informações pessoais de cada arquivo talvez não consistam apenas de dados brutos, mas também de informações subjetivas, como opiniões ou instruções. Os dados podem também vir de fontes que não sejam o indivíduo, incluindo fontes protegidas. No entanto, a divulgação de tais informações pode ser prejudicial para o indivíduo ou outras pessoas.

A maioria dos instrumentos internacionais reconhece restrições de acesso aos dados pessoais. Todas as legislações nacionais também preveem restrições desse direito. A *Lei de Proteção de Dados Pessoais* da Suíça estabelece que tais informações podem ser retidas se a lei assim determinar ou se interesses primordiais de terceiros o exigirem. Órgãos federais também podem restringir o acesso aos dados pessoais se isto for do interesse público ou se o acesso puder pôr em risco uma investigação criminal. No entanto, as exceções ao requisito do acesso devem ser limitadas e específicas, e as razões para negar o acesso devem ser informadas ao indivíduo mediante pedido. A *Lei de Privacidade* canadense estabelece como exceções ao direito do acesso: informações pessoais obtidas confidencialmente, informações relativas a relações internacionais, defesa, aplicação da lei, investigação e dados que razoavelmente se espera que possam ameaçar a segurança de indivíduos. Entre as exceções razoáveis, portanto, incluem-se informações que:

- contêm referências a outros indivíduos ou fontes de informação recebidas confidencialmente;
- poderia-se razoavelmente esperar que sejam prejudiciais ao interesse público (segurança nacional, ordem pública, etc.);
- poderia-se razoavelmente esperar que sejam altamente prejudiciais aos interesses de outras pessoas;
- poderiam impedir ou comprometer a finalidade para a qual foram coletadas.

Se os dados de um titular que fez um pedido de acesso puderem ser separados das informações relativas a outras pessoas ou de informações que não podem

ser divulgadas, não é necessário negar o acesso a todas as informações. No entanto, se os dados não puderem ser separados, o órgão que os mantém terá de encontrar um equilíbrio entre os interesses envolvidos ao considerar a divulgação das informações. Deverá inclusive buscar um equilíbrio entre os interesses do titular e os das outras pessoas caso as informações também se refiram a elas, ou o interesse público, conforme o caso.

Com relação a determinados tipos de informações, podem-se aplicar condições especiais. Alguns atos legislativos nacionais exigem que os dados médicos sensíveis sejam disponibilizados através de um médico (por exemplo, Suíça) ou que não sejam divulgados quando tal for contrário ao interesse superior do indivíduo (como no Canadá).

As *Diretrizes* das Nações Unidas preveem o direito de acesso somente do titular, mas reconhecem que pode haver exceções permitindo que terceiros tenham acesso aos dados caso isso seja necessário para proteger o interesse público (segurança nacional, ordem pública, etc.) ou, inter alia, os direitos e liberdades de outros, desde que as exceções sejam expressamente especificadas na lei.

De acordo com a *Lei de Proteção de Dados Pessoais* da Argentina, o direito de acesso aos dados pessoais só pode ser exercido pelo titular ou pelo seu tutor. Se o titular estiver morto, o direito de acesso pode ser exercido pelos herdeiros. A lei suíça não prevê direito de acesso a ninguém que não seja o titular. No entanto, os órgãos federais podem transmitir dados pessoais a terceiros caso o titular tenha dado consentimento ou se, de acordo com as circunstâncias, tal consentimento possa ser presumido. A *Lei de Privacidade* canadense estabelece que o chefe de uma instituição governamental pode se negar a divulgar qualquer dado pessoal sobre outro indivíduo, o que pareceria indicar que as informações sobre outro indivíduo podem ser divulgadas em determinadas circunstâncias. A regra básica é que os dados pessoais sob o controle de uma instituição governamental podem não ser divulgados sem o consentimento do titular, salvo em circunstâncias especificadas. Entre as exceções, incluem-se: a divulgação para o objetivo pelo qual as informações foram obtidas ou compiladas; e a divulgação para qualquer objetivo se, na opinião do chefe da instituição, claramente beneficiar o titular. Portanto, a menos que se considere que a divulgação das informações aos familiares figure em uma destas últimas categorias, ou a menos que o consentimento seja presumido, as informações pessoais não serão divulgadas aos familiares.

Por motivos humanitários – ajudar a localizar pessoas desaparecidas e restos mortais –, pode ser então necessário que a legislação sobre proteção de dados em alguns Estados seja modificada para permitir o acesso de terceiros a tais informações. Disposições da legislação sobre proteção de dados que permitem a divulgação “no interesse público” podem ser vagas demais para garantir que terceiros que tentam localizar pessoas desaparecidas possam obter acesso às informações necessárias. Entre esses terceiros, podem-se incluir familiares ou outras pessoas legitimamente interessadas em ajudar a localizar a pessoa. De modo alternativo, a legislação em matéria de liberdade de informação poderia ser modificada para permitir que certos indivíduos tenham direito de acesso aos dados sobre pessoas desaparecidas, se for do interesse do desaparecido ou de familiares, ou ainda se for de interesse público.

Outra maneira de permitir que os familiares tenham acesso seria considerá-los como representantes da pessoa desaparecida. Desse modo, poderiam agir no lugar dessa pessoa e obter acesso às informações sobre ela.

Deve-se também observar que a Suprema Corte da Argentina considerou, no contexto do acesso a informações mantidas por autoridades públicas, que os dados relativos à sorte de um familiar (no caso em questão, um irmão) que foi vítima de desaparecimento forçado poderiam ser considerados dados pessoais e, portanto, sujeitos ao direito de acesso. Um tribunal superior brasileiro, no entanto, adotou a visão contrária.

2.2. Identificação de restos mortais

PRINCÍPIO 1

A autoridade pública competente deve estabelecer a identidade dos restos mortais e a causa da morte com a devida diligência.

Na maioria das legislações nacionais, a morte deve ser comunicada a um escrivão ou funcionário do registro civil pela pessoa responsável por registrá-la, normalmente um familiar da pessoa falecida ou, se não houver familiares vivos, qualquer pessoa capaz de identificá-la. Se a pessoa falecida não puder ser identificada, a certidão de óbito deve incluir uma descrição do corpo e das circunstâncias da descoberta. O corpo pode receber o tratamento final uma vez que o escrivão tiver emitido o certificado adequado. Podem-se impor mais requisitos em caso de cremação.

Os propósitos da certificação da morte são: confirmar que esta ocorreu; indicar a sua causa provável; apoiar as pessoas interessadas se a causa for contestada; garantir que as mortes sejam investigadas antes do tratamento final dos restos mortais caso tenha início uma ação penal; e fornecer dados estatísticos sobre as causas da morte. Na maioria dos casos, a lei exige que um médico preencha as informações contidas no atestado de óbito. Em alguns casos, se a morte for óbvia e não puder ser atestada por um médico em um prazo razoável, poderá ser certificada pela Justiça de Paz (por exemplo, *Código Civil*, Quebec, Canadá, artigo 123).

Antes que a morte possa ser registrada e que o corpo receba um tratamento final, um médico deve normalmente preencher uma declaração com a causa da morte. Se a causa parece ter sido não natural, súbita e desconhecida, ou provocada por violência, a morte geralmente deve ser comunicada às autoridades. Como regra geral, toda pessoa que encontrar um corpo tem o dever, logo que possível, de informar a polícia (por exemplo, *Lei relativa a Coroners*¹⁰, Nova Zelândia, artigo 5)

Na maioria dos países do *Common Law*¹¹ as mortes suspeitas devem ser informadas a um *coroner* ou um médico legista (por exemplo, *Leis Gerais* de Massachusetts, EUA, capítulo 38, seção 3; *Lei relativa a Coroners* Nova Zelândia, seção 4; *Lei relativa à determinação das causas e circunstâncias da morte*, Quebec, Canadá, artigos 34-36). Isto normalmente é feito pelo médico que emite o atestado de óbito ou pela polícia. O *coroner* é um funcionário judicial independente encarregado de investigar as circunstâncias de determinadas categorias de morte para a proteção da população. O inquérito do *coroner* é um exercício de investigação. Não é um julgamento e não tem como objetivo estabelecer responsabilidade civil ou penal. O *coroner* tem a responsabilidade final de identificar as pessoas falecidas, sendo também encarregado de estabelecer a causa e a hora da morte. As responsabilidades da polícia em nome do *coroner* incluem o controle, a identificação e a entrega dos restos mortais a um familiar com o consentimento do *coroner*.

De acordo com a *Lei relativa a Coroners* de 1988, do Reino Unido, “quando um *coroner* é informado de que um corpo (a pessoa falecida) se encontra em seu distrito e existem motivos razoáveis para suspeitar que a pessoa: a) teve morte violenta ou não natural; b) teve morte súbita cuja causa é desconhecida; ou c) morreu na prisão ou em um lugar ou circunstância que exija um inquérito

10 A figura do “*coroner*” não tem um equivalente no Brasil. Para fins desta tradução, decidiu-se manter o termo em inglês, cujo significado seria “funcionário público que investiga a identidade da pessoa falecida e as circunstâncias de uma morte que ocorra de forma não natural ou violenta”.

11 O termo *common law* se refere a um sistema jurídico de normas e regras não escritas, mas, sim, sancionadas pelo costume ou pela jurisprudência

de acordo com qualquer outra Lei, então o coroner deve, assim que possível, iniciar um inquérito sobre essa morte" (artigo 8º).¹² A finalidade da investigação do coroner é estabelecer, na medida do possível ou na medida em que possa ser provado, que a pessoa morreu, a identidade dela, quando e onde morreu, assim como a causa e as circunstâncias da morte (por exemplo, *Lei relativa a Coroners*, Nova Zelândia, artigo 15, *Lei relativa a Coroners*, Reino Unido, artigo 11). A Lei de Quebec exige que o coroner identifique todos os corpos desconhecidos, confirme as identidades presumidas e estabeleça a causa e a forma da morte. Em outras províncias canadenses, mortes suspeitas ou não naturais são investigadas por coroners ou médicos legistas. Nos Estados Unidos, as investigações sobre mortes variam consideravelmente conforme a jurisdição. Algumas jurisdições utilizam o sistema médico-legal; já outros seguem o sistema do coroner (os legistas normalmente são nomeados, enquanto os coroners são eleitos). Os legistas e os coroners são responsáveis por investigar casos de morte súbita ou violenta. As mortes a serem investigadas variam segundo a jurisdição, mas normalmente incluem casos repentinos, suspeitos ou inexplicáveis, incluindo a identificação de cadáveres desconhecidos (por exemplo, *Leis Gerais* de Massachusetts, EUA, cap. 38, artigo 2º).

A Seção 74 do *Código de Processo Penal* da França estabelece que:

"Quando um corpo é descoberto, se a causa da morte for desconhecida ou suspeita, independentemente de ser violenta, o oficial da polícia judiciária em questão informará imediatamente o promotor público, visitará imediatamente o lugar da descoberta e fará um relatório inicial. O promotor público visitará o lugar se considerar necessário e requisitará a assistência de pessoas capazes de avaliar a natureza das circunstâncias da morte. Para isto, ele pode também delegar responsabilidades a um oficial da polícia judiciária da sua escolha [...]"¹³

Uma investigação sobre a causa da morte pode também ser obrigatória de acordo com os instrumentos de direitos humanos. A Corte Europeia e a Corte Interamericana de Direitos Humanos estabelecem que a proteção conferida pelo direito à vida envolve a determinação da causa da morte (ver *McCann vs. Reino Unido*, 1996, 21 EHRR 97).

PRINCÍPIO 2

Durante uma investigação ou inquérito, inclusive na decisão de realizar um exame post mortem, devem-se considerar as opiniões crenças religiosas da pessoa falecida e seus familiares.

No caso de morte suspeita ou descoberta de um cadáver, ou ainda quando a certidão de óbito mencionar um empecilho ao sepultamento, a maioria das legislações nacionais estabelece que o corpo deve permanecer à disposição das autoridades judiciais ou investigadoras durante o tempo necessário.

Segundo a legislação francesa, o corpo permanece à disposição das autoridades judiciais e o atestado de óbito é transmitido ao promotor público. Os ritos funerários são suspensos até que a autoridade judicial os autorize, normalmente após um exame *post mortem*. Pareceria que, de acordo com um princípio de ordem pública, não se pode objetar a busca da verdade, isto é, o estabelecimento da causa da morte. Um exame *post mortem* pode ser ordenado pelo Ministério Público ou um juiz de instrução em casos de morte suspeita ou violenta (crime, suicídio ou acidente).

¹² Tradução livre do CICV.

¹³ Tradução livre do CICV.

Nos países do *Common Law*, pode-se realizar um exame *post mortem* quando o *coroner* tiver de realizar um inquérito sobre uma morte ou tiver iniciado um inquérito sem concluí-lo, ou ainda para permitir que o *coroner* decida se deve realizar tal investigação. Os tribunais reconheceram que o *coroner* tem o direito absoluto de posse e controle do corpo a partir do momento em que recebe uma denúncia sobre um assassinato até a conclusão do inquérito. Normalmente, não existe qualquer exigência legal de que seja obtido consentimento de pessoa natural ou jurídica para a realização de um inquérito, exame *post mortem* ou exame especial. Estes, portanto, devem ser feitos mesmo se não houver consentimento e até mesmo apesar da objeção de familiares. Os tribunais também aprovaram a prática dos *coroners* de reter o corpo para a realização do exame *post mortem*.

Na legislação dos Estados Unidos, tecidos ou outras partes do corpo não podem ser removidos do cadáver para análise forense ou científica sem o consentimento da pessoa que tem o dever de sepultá-lo (por exemplo, o cônjuge ou um familiar), exceto com autorização legal. Essa autorização e o poder de ordenar uma autópsia são geralmente conferidos a *coroners*, médicos-legistas ou procuradores-gerais para a investigação de mortes suspeitas ou a identificação de restos mortais (por exemplo, *Leis Gerais* de Massachusetts, cap. 38, artigo 4º).

Em muitos territórios australianos, a menos que o *coroner* considere que se deva realizar um exame *post mortem* imediatamente, o “familiar mais velho” da pessoa falecida poderá se opor (por exemplo, *Lei relativa a Coroners* de 1993, Território do Norte, artigo 23; *Lei relativa a Coroners* de 1985, Vitória, artigo 29). Se o *coroner* decidir que tal exame é necessário, ele deve notificar o familiar mais velho e só realizá-lo 48 horas após a notificação. Isto permite que o familiar recorra à Justiça para tentar impedir o exame *post mortem*. Os tribunais australianos resolveram que se devem levar em conta as crenças religiosas e que, em determinadas circunstâncias, o direito do familiar de ser poupado de maiores sofrimentos supera o interesse comunitário em descobrir a verdadeira causa da morte (*Green vs. Johnstone*, [1995] 2 VR 176 (Suprema Corte de Vitória, Austrália); *Re Death of Simon Unchango (filho)*, *ex parte Simon Unchago (pai)*, (1997) 95 A. Crim. R. 65; nos casos envolvendo a morte de crianças, as mortes não ocorreram em circunstâncias suspeitas). Um tribunal de apelação australiano considerou que, se um *coroner* estiver ciente dos pontos de vista da família, ele deve levá-los em conta.

Podem-se encontrar princípios similares na *Lei relativa a Coroners* da Nova Zelândia. Ao decidir se autoriza ou não o exame, o *coroner* deve considerar, entre outras coisas:

- “a conveniência de minimizar a angústia causada às pessoas que, pelas suas origens étnicas, costumes, atitudes e hábitos sociais ou crenças religiosas, habitualmente pedem que os corpos estejam à disposição dos familiares assim que possível após a morte;
- a conveniência de minimizar a possibilidade de ofender pessoas que, devido às suas origens étnicas, costumes, atitudes sociais ou crenças religiosas, consideram ofensivo o exame *post mortem* dos corpos;
- o desejo de qualquer um dos familiares mais próximos da pessoa em questão de que o exame *post mortem* seja realizado (artigo 8º).¹⁴

De acordo com a legislação de Quebec, um exame *post mortem* realizado para determinar a identidade da pessoa falecida ou a causa da morte não requer consentimento dos familiares. O Código de Ética dos *Coroners*, no entanto, estabelece que as opiniões e crenças religiosas da pessoa e dos seus familiares devem ser respeitadas na medida em que os requisitos impostos por lei assim o permitirem.

14 Tradução livre do CICV.

PRINCÍPIO 3

Ao determinar a causa e as circunstâncias da morte, em especial durante uma investigação ou inquérito, devem-se respeitar a honra, dignidade, reputação e privacidade da pessoa falecida. Devem-se tratar com dignidade e respeito todos os corpos sob custódia e em poder de uma autoridade investigadora.

As legislações e tribunais nacionais reconhecem que as pessoas falecidas devem ser tratadas com decência e respeito, de acordo com as expectativas morais da comunidade. A maioria das normas nacionais estabelece que um órgão não deve ser submetido a qualquer exposição, procedimento ou tratamento desnecessário ou não autorizado que seja incompatível com os desejos da pessoa falecida ou da sua família. Isto também se reflete nos códigos de ética dos funcionários públicos e/ou médicos. O Código de Ética dos *Coroners* do Quebec estabelece que o corpo será tratado com dignidade e respeito. O *Código de Ética Médica* da França afirma que “o médico, cujo dever é a saúde pública e do indivíduo, cumprirá sua missão com respeito pela vida humana, pelo indivíduo e por sua dignidade. O respeito pela pessoa deve continuar mesmo após a morte”.¹⁵

A maioria das legislações penais considera que é um delito provocar uma alteração indevida e indecente em um cadáver. De acordo com o *Código Penal* do Canadá e o de Queensland (Austrália), toda pessoa que interferir de maneira indevida ou indecente ou realizar qualquer ato indigno em corpos humanos ou restos mortais, sepultados ou não, estará sujeita a pena de prisão. De acordo com o artigo 262 do *Código Penal* da Suíça, “toda pessoa que insultar publicamente ou abusar de um corpo humano estará sujeita a pena de reclusão ou multa”.¹⁶ O *Código Penal* da França estabelece que “qualquer ataque contra a integridade do corpo, por qualquer meio, será punido com um ano de reclusão ou multa de 15 mil euros” (art. 225-17).¹⁷

PRINCÍPIO 4

As exumações devem ser autorizadas pela autoridade competente.

Na maioria dos países, a exumação está sujeita a uma variedade de normas relativas ao sepultamento, às leis eclesiais e à proteção da saúde.

Em geral, as exumações precisam de autorização. Na maioria dos Estados, elas podem ser autorizadas pelos funcionários locais ou por decisão de um juiz para fins de inquérito judicial. A lei belga sobre funerais e enterros estabelece, por exemplo, que “cemitérios (e crematórios) comunitários estão sujeitos às autoridades, à polícia e à vigilância das autoridades comunitárias, que garantirão que não seja cometido nenhum ato de desordem ou desrespeito pela memória dos mortos e que nenhum corpo seja exumado sem autorização”.¹⁸ Segundo a legislação da Malásia, a exumação pode ser autorizada por um tribunal ou mediante licença concedida pelas autoridades locais (*Lei relativa a Governos Locais*, 1976). A legislação que regula a atividade dos *coroners* nos países do *Common Law* normalmente estabelece que esse profissional pode ordenar uma exumação quando razoavelmente acreditar que possa ser útil para o desempenho dos seus deveres.

15 Tradução livre do CICV.

16 *Idem*

17 *Idem*

18 *Idem*.

Na maioria dos sistemas nacionais, podem-se realizar exumações nas seguintes circunstâncias: a) por ordem de um tribunal ou um juiz em casos cíveis (por exemplo, em casos de filiação parental); b) a fim de sepultar um corpo em outro lugar ou restaurar o túmulo; e c) por ordem de um funcionário público cujo dever é determinar a identidade da pessoa falecida ou a causa da morte (por exemplo, *Código Civil*, Quebec, Canadá, artigo 49; *Lei relativa a Coroners*, Vitória, Austrália, artigo 30).

PRINCÍPIO 5

A decisão de realizar uma exumação deve levar em conta os interesses do familiar mais próximo.

Normalmente, é o familiar mais próximo que solicita a exumação. O pedido é em geral apresentado às autoridades civis ou eclesiásticas locais, dependendo do lugar de sepultamento. Na Bélgica e na França, os funcionários locais concedem uma autorização para as exumações. No Reino Unido, o Ministério do Interior emite uma autorização para o procedimento, enquanto a Arquidiocese outorga uma licença caso os restos mortais sejam sepultados em terrenos consagrados. O funcionário local muitas vezes tem margem para decidir, a seu critério, se concede a permissão. Ele deve levar em consideração o devido respeito pelos mortos e a manutenção da ordem pública. Outros familiares também podem se opor à exumação. Disputas entre o requerente e a autoridade local, ou entre familiares, podem ser levadas perante tribunais civis ou administrativos, conforme o caso.

O consentimento do familiar geralmente não é necessário quando a exumação é ordenada por um investigador, um magistrado ou um juiz. No entanto, as *Leis relativas a Coroners* de Vitória, Austrália Ocidental e Tasmânia (Austrália) estabelecem que o *coroner* deve notificar o “familiar mais velho” da pessoa falecida e os administradores ou donos do cemitério ou do lugar de sepultamento antes que o corpo seja exumado, a menos que isso não seja

Familiares de pessoas desaparecidas olham as fotos e registros de arquivos durante encontro com funcionários do CICV.



possível. Se o familiar mais velho se opuser à exumação, o corpo não deverá ser exumado nas 48 horas posteriores ao pedido. Isto permitirá que o familiar recorra à Justiça para tentar impedir a exumação.

Nenhuma legislação nacional exige a presença de familiares. Em geral, só é necessária a presença do funcionário público ou do magistrado que ordenou a exumação e de um médico legista. Quando um familiar próximo solicita a exumação, a legislação francesa exige a presença de um familiar ou um representante da família. No Reino Unido, por outro lado, os familiares normalmente não são autorizados a presenciar a exumação.

As legislações nacionais sobre exumações geralmente são formuladas para aplicação em circunstâncias ordinárias. Métodos e procedimentos específicos podem ser mais adequados em situações de conflito armado ou violência interna, quando é preciso confirmar a identidade do corpo a ser exumado ou quando os cadáveres devem ser desenterrados de valas comuns. As famílias ou a comunidade, conforme o caso, devem ser mais estreitamente envolvidas no processo de exumação em tais situações, de modo a facilitar a aceitação do procedimento e dos resultados.

PRINCÍPIO 6

As exumações devem ser realizadas de acordo com os padrões reconhecidos, incluindo as normas de proteção da saúde.

A maioria das normas da legislação nacional exige a observância dos requisitos estabelecidos pelas autoridades de saúde. De acordo com a legislação australiana, todas as exumações devem cumprir com as condições estipuladas pelos departamentos de saúde, tais como o Departamento de Saúde e Assistência Comunitária do Território da Capital Australiana. Tais normas preveem procedimentos de proteção da saúde pública e das pessoas que realizam a exumação (por exemplo, roupas de proteção, uso de desinfetantes, etc.). Além disso, as exumações devem ser realizadas sob a supervisão de uma autoridade da saúde pública. No Reino Unido, exige-se a presença de um agente da saúde pública. A lei de Newfoundland (Canadá) determina que as exumações sejam realizadas de acordo com as recomendações do Ministério da Saúde (*Lei de Exumações*, artigo 2º). O *Código dos Municípios* francês exige que se tome uma série de precauções de saúde.

PRINCÍPIO 7

As famílias devem ser informadas sobre as decisões tomadas referentes aos exames post mortem, assim como dos resultados de qualquer análise desse tipo

Embora não se exija o consentimento dos familiares, determinadas pessoas e agências devem ser notificadas sobre a data e a hora do exame *post mortem* proposto, a menos que seja impraticável ou cause uma demora indevida; isto inclui "qualquer familiar da pessoa falecida que tenha notificado o *coroner* sobre o seu desejo de comparecer ou ser representado no exame *post mortem*" (Norma 7(2)(a), Normas 1984, Reino Unido).¹⁹ O *coroner* tem poder para notificar, a seu critério, qualquer outra pessoa a qual não tenha o dever de notificar. As *Notas de Prática para Coroners*, emitidas pela Sociedade de *Coroners* do Reino Unido, estabelecem que os familiares da pessoa falecida devem receber informações adequadas sobre um *post mortem* proposto.

¹⁹ Tradução livre do CICV.

De modo similar, o *Código de Ética dos Coroners* do Quebec estipula que o *coroner* deve proporcionar informações aos familiares da pessoa falecida, caso seja necessário. No Reino Unido, o *Memorando sobre Boas Práticas* do Ministério do Interior também estabelece que a família da vítima deve ser mantida informada sobre os procedimentos e receber o apoio apropriado. O familiar mais próximo deve também ser avisado quando o laudo do *coroner* estiver disponível. A *Carta Modelo de Serviço do Coroner* do Reino Unido determina que, se for necessário um exame *post mortem*, o familiar mais próximo deve saber o motivo e o contexto, caso o solicite. Deverá também receber uma notificação prévia sobre os preparativos, se isto for viável, e uma cópia do exame *post mortem* se a pedir.

A *Lei relativa a Coroners* de 1988 da Nova Zelândia estabelece que um *coroner* que tenha autorizado um exame *post mortem* tomará, tão logo seja possível após a sua realização, todas as medidas razoáveis para assegurar que um membro da família imediata da pessoa em questão seja avisado de que o exame foi autorizado e as razões do *coroner* para autorizá-lo. Qualquer membro da família da pessoa falecida pode obter uma cópia do laudo do exame, por parte do *coroner*, após sete dias (artigo 11).

O laudo do exame *post mortem* é entregue ao *coroner* e não pode ser divulgado a qualquer outra pessoa sem o seu consentimento. O *coroner* deve fornecer uma cópia do documento a qualquer um que, na sua opinião, seja uma “pessoa devidamente interessada” (mediante pagamento de taxa), mas não há exigência legal para que os familiares recebam uma cópia do laudo do exame ou uma notificação do resultado do inquérito. As *Notas de Prática* estipulam, no entanto, que “os familiares da pessoa falecida [...] devem saber o resultado do exame assim que possível e por escrito, se o solicitarem [...]. Pode ser apropriado oferecer o encaminhamento do resultado e uma cópia do laudo do exame do patologista ao médico designado pelos familiares, que lhes poderá explicá-los”²⁰

Em algumas situações, os familiares podem não querer ser informados das circunstâncias da morte, já que isto poderia lhes causar sofrimento desnecessário. Essa dificuldade pode ser resolvida com o envio das informações ao médico da família, que poderá explicar as circunstâncias da morte, ou com a omissão de dados que a família pode não querer conhecer.

PRINCÍPIO 8

Os restos mortais devem ser restituídos aos familiares o quanto antes.

O princípio aceito é que não há direito de propriedade sobre o cadáver. De fato, é uma antiga norma do *Common Law* a de que não há direito de propriedade sobre o cadáver. (*Williams vs. Williams* (1880) 20 Ch. D. 659). O *Código Civil* francês reconhece, de modo similar, que “o corpo humano, os seus componentes e produtos não dão lugar a um direito de propriedade” (*Código Civil*, França, art. 16-1).²¹

Uma vez concluído o inquérito, o *coroner* ou médico legista já não tem o direito de reter o corpo, que deve ser restituído aos seus possuidores legítimos. O *Common Law* reconhece que os familiares da pessoa falecida têm o direito de posse sobre o corpo, correspondente ao dever de providenciar o tratamento final adequado. Esse dever cabe principalmente ao representante da pessoa que faleceu. Se nenhum testamenteiro tiver sido nomeado, a primeira pessoa com direito a lidar com a herança da pessoa falecida terá direito de posse. Entre as outras pessoas encarregadas por lei de sepultar o corpo incluem-se, por

²⁰ Tradução livre do CICV.

²¹ Idem.

exemplo, o pai de uma criança que morre, quando esse pai tem os meios para fazê-lo. Como o direito de posse decorre do dever de dar um tratamento final ao corpo, este só pode ser reivindicado com tal finalidade.

Nas situações em que os segmentos corporais tenham se espalhado e não tenham sido recuperados ao mesmo tempo, deve-se comunicar o fato à família e lhe perguntar se deseja ser informada da recuperação de distintos restos mortais assim que a identificação for definitivamente confirmada. Para poupar as famílias de mais sofrimento, os procedimentos para a identificação das vítimas do ataque contra o *World Trade Center* incluíram dar a elas a opção de deixarem quaisquer restos mortais identificados no instituto médico legal até que os testes terminassem (um único sepultamento poderia então ser realizado) ou de serem notificadas apenas quando a confirmação final tivesse sido feita.

Os atrasos na liberação dos restos mortais quando um exame *post mortem* deve ser realizado têm sido motivo de preocupação para as famílias das vítimas, em especial em casos de crime, quando o réu pode solicitar um segundo exame *post mortem*. Uma circular do Ministério do Interior do Reino Unido sobre esse tipo de análise e a liberação antecipada de corpos contém um memorando de boas práticas que se baseia nas seguintes considerações:

- deve-se fazer todo esforço para que uma decisão sobre a necessidade de um segundo exame *post mortem* seja tomada o mais breve possível;
- quando ninguém tiver sido acusado em conexão com a morte no prazo de um mês, serão tomadas medidas para a realização de um segundo e independente exame *post mortem* a ser usado por um réu no futuro, se necessário;
- o corpo será liberado para sepultamento ou cremação o quanto antes;
- pedidos de múltiplos exames feitos de maneira conjunta por réus serão considerados criticamente;
- todos os indivíduos e agências envolvidos tentarão minimizar a demora, conforme o prazo máximo recomendável.

A *Lei relativa a Coroners* de 1988 da Nova Zelândia enfatiza a importância de liberar o cadáver o mais rápido possível. Estabelece também que, tão logo o *coroner* considerar que já não é necessário reter o corpo com relação aos familiares, autorizará imediatamente o seu tratamento final (artigo 14). A lei permite que o *coroner* instrua o médico a realizar prontamente um exame *post mortem* caso os familiares da pessoa falecida tenham origem étnica, costumes, atitudes sociais ou crenças religiosas que habitualmente requerem que os corpos estejam disponíveis à família assim que possível após a morte (artigo 9º).

De modo análogo, o *Código de Ética do Coroner* do Quebec estabelece que a liberação do corpo será facilitada com toda a diligência que os familiares possam esperar de modo razoável. A *Lei relativa à Determinação das Causas e Circunstâncias da Morte*, do Quebec, determina que exames *post mortem* sejam realizados com a devida diligência.

PRINCÍPIO 9

Deve-se recompôr o cadáver antes da sua restituição aos familiares, que devem ser notificados caso houver retenção de segmentos corporais.

Um exame *post mortem* tipicamente envolve um exame da parte externa do corpo. Pequenas amostras de tecidos podem ser obtidas para análise. Os segmentos corporais podem ser cortados a fim de estabelecer a identidade ou a causa da morte. A remoção de órgãos pareceria também ser um procedimento normal no exame *post mortem* do *coroner*, sobretudo para estabelecer a causa da morte; o coração e o cérebro, em particular, podem ser retidos e talvez não

estejam disponíveis com o restante do corpo para o sepultamento ou cremação. Blocos e lâminas de tecido também são normalmente coletados e conservados. Os *coroners* em geral não precisam notificar ou obter consentimento da família da pessoa falecida caso tenham de remover e conservar segmentos corporais. De modo similar, o *Código de Saúde Pública* francês estabelece que “não pode haver remoções para fins científicos sem o consentimento da pessoa falecida expressado diretamente ou através da família, salvo as realizadas para estabelecer a causa da morte” (*Código de Saúde Pública*, França, art. L1232-3).²²

Os tribunais dos Estados Unidos há muito consideram que o direito dos familiares ao corpo de uma pessoa falecida “é o direito ao que resta quando a respiração deixa o corpo, não meramente a esse cadáver cortado, decepado e mutilado que algum desconhecido, um infrator da lei penal, pode resolver entregar a um familiar aflito” (*Burney vs. Children’s Hosp.*, 1897).²³

Uma vez concluída a autópsia, os segmentos corporais que não forem retidos devem ser reconstituídos ao cadáver, que por sua vez deve ser recomposto antes de ser liberado. Na Austrália do Sul, o diretor do funeral é obrigado a certificar que o corpo foi entregue em condições apropriadas. O *Código de Saúde Pública* francês afirma que “médicos que removem uma parte do cadáver são obrigados a assegurar a reconstrução decente do corpo” (*Código de Saúde Pública* (França), art. L1232-5).²⁴

O *Common Law* não é claro sobre se cada segmento corporal que possa ser descoberto – por exemplo, após um acidente ou após o enterro do restante do corpo, ou mesmo cada lâmina e amostra de tecido obtida em um laboratório de patologia após um exame *post mortem* – deve ser considerada dentro da definição de “corpo” no cumprimento do dever de dar um tratamento final digno aos restos mortais. Não se sabe, portanto, se o direito de reivindicar a posse de um corpo em cumprimento com o dever de dar um tratamento final digno estende-se aos segmentos corporais. Os tribunais britânicos e australianos reconheceram, em circunstâncias limitadas, uma exceção à regra do *Common Law* de que um cadáver ou parte dele poderia não ser propriedade quando o corpo ou parte dele tenha sido alterado pela aplicação de perícia. Uma recente decisão da Suprema Corte da Austrália Ocidental determinou que uma amostra de tecido cirúrgico conservado por um laboratório de patologia era de sua propriedade. Tratava-se de saber se a Corte poderia ordenar que a amostra de tecido de uma pessoa falecida fosse utilizada em testes de DNA para estabelecer se a autora da ação era filha natural dessa pessoa (*Roche vs. Douglas*). A extensão da perícia que deve ser utilizada para que um direito de posse ou propriedade sobre um tecido seja aplicado à pessoa que realiza a perícia, no entanto, é incerta. Quando existe um direito de propriedade sobre uma parte relevante do corpo, já não há qualquer obrigação de sepultá-la. Portanto, os familiares não teriam o direito de reivindicar a posse para fins de enterro.

Uma vez autorizada a realização do exame *post mortem*, as legislações nacionais de alguns países permitem a retenção de segmentos e tecidos corporais retirados para o próprio exame, transplante ou para fins científicos, médicos ou terapêuticos. Outras não o permitem.

O artigo 8.o da *Convenção Europeia de Direitos Humanos* é interpretado no sentido de proteger o indivíduo contra a ingerência arbitrária das autoridades públicas na sua vida privada ou familiar. O conceito de “vida familiar” é amplamente interpretado, embora ainda não tenha sido determinada a questão de se a retirada, retenção e utilização de tecido de um familiar da pessoa falecida possa ser uma interferência na vida familiar.

22 Tradução livre do CICV.

23 *Idem*.

24 *Idem*.

2.3 Proteção de informações genéticas

PRINCÍPIO 1

A coleta, o uso e a divulgação de perfis de DNA estão sujeitos a normas relativas à proteção de dados pessoais.

Os perfis de DNA contêm informações pessoais que são reguladas por textos nacionais e internacionais. A maioria das autoridades nacionais responsáveis pela proteção de dados pessoais que examinaram a questão dos bancos de dados de DNA sustenta que a legislação nacional relativa à proteção de informações pessoais é aplicável à gestão, à utilização e ao armazenamento de amostras e perfis de DNA.

Em alguns casos, adotaram-se disposições específicas sobre a questão na legislação nacional. O projeto de lei suíço sobre o uso de perfis de DNA estabelece especificamente que o acesso às informações de DNA está sujeito às disposições da *Lei Federal sobre Proteção de Dados*, assim como a transferência de dados de DNA para o exterior.

A gestão do banco de dados de DNA criado em âmbito federal na Austrália é da responsabilidade de uma agência executiva sujeita à *Lei de Privacidade* australiana.

PRINCÍPIO 2

A identificação dos restos mortais por tipagem de DNA só deve ser realizada quando outros métodos investigativos de identificação não forem adequados.

Utiliza-se uma série de técnicas de investigação para identificar restos mortais com base em características do esqueleto, radiografias dentais e impressões digitais. Podem-se obter provas secundárias a partir de roupas e pertences pessoais. No entanto, os restos mortais sujeitos à violência da guerra moderna ou aos danos causados pelo tempo podem já não ser adequados para os meios tradicionais de identificação. Quando os restos biológicos não podem produzir evidências dentárias e de impressões digitais, a tipagem de DNA pode fornecer provas adicionais para apoiar a identificação.

A análise de perfis de DNA só pode ser utilizada para confirmar a identidade de uma pessoa quando familiares de grau mais próximo estejam disponíveis para fornecer uma amostra, que será comparada com as do corpo, salvo quando estiverem disponíveis amostras *ante mortem*. A fim de evitar sofrimento à família, os perfis de DNA só devem ser considerados como um último recurso quando todos os outros métodos de identificação tenham se mostrado infrutíferos. Esse princípio é reconhecido, por exemplo, no projeto de lei suíço sobre o uso de perfis de DNA.

PRINCÍPIO 3

As amostras de DNA só podem ser obtidas e analisadas com o consentimento informado do indivíduo, salvo quando um interesse público superveniente exigir o contrário.

A exigência do consentimento do indivíduo é compatível com o princípio do consentimento para a coleta de dados pessoais. Também é compatível com a proteção da privacidade tal como asseguram os instrumentos internacionais de direitos humanos.

A menos que as amostras sejam obtidas de suspeitos no decurso de uma investigação criminal ou de pessoas condenadas, a coleta de amostras e a análise de DNA exigem o consentimento do indivíduo em questão na maioria das legislações nacionais. Uma exceção ao princípio geral do consentimento fora de uma ação penal é a obrigação dos membros das forças armadas dos Estados Unidos de fornecer amostras de DNA, que tem sido contestada sem êxito perante os tribunais.

O *Relatório Explicativo da Recomendação R (92) 1* do Conselho da Europa observa que há uma importante diferença entre as abordagens dos países do *Common Law* e os da Europa continental com relação à exigência do consentimento. Nos países continentais, se o consentimento for negado, uma ordem judicial pode normalmente obrigar a coleta de uma amostra em determinadas circunstâncias. Nos países do *Common Law* (por exemplo, o Reino Unido), se o consentimento for negado não se pode obrigar a coleta de amostras íntimas; a recusa, no entanto, pode ir em detrimento da pessoa que retirou o consentimento. Na prática, contudo, pode não haver diferença, já que há relatórios indicando que suspeitos ou detentos foram colocados sob pressão para dar consentimento à coleta de amostras em muitos países.

No caso de uma pessoa desaparecida, é necessário o consentimento de familiares consanguíneos, mas não da pessoa desaparecida (seu representante ou familiares). O projeto de lei suíço sobre o uso de perfis de DNA permite a análise de material biológico coletado de alguém que desapareceu caso o perfil seja necessário para a identificação. O perfil de DNA de familiares consanguíneos de pessoas desaparecidas também pode ser estabelecido, com o consentimento deles.

Poucos países dispõem de legislação nacional com orientações precisas sobre o consentimento e sobre as informações a serem fornecidas à pessoa que voluntariamente se submete a uma análise forense. A maior parte da legislação dos Estados Unidos determina, no entanto, que a pessoa submetida a um procedimento desse tipo deve ser informada sobre ele (de que forma a amostra será coletada) e que as informações devem ser armazenadas em um banco de dados de DNA. Com base nas normas gerais sobre a coleta de dados pessoais, as seguintes informações devem ser fornecidas à pessoa que voluntariamente realiza uma análise forense para que o seu consentimento seja informado:

- a maneira em que a análise forense será realizada;
- que a pessoa não é obrigada a se submeter ao procedimento;
- que a pessoa pode, em qualquer momento, retirar o consentimento para: a) submeter-se à análise forense; ou b) a retenção do material forense coletado ou das informações obtidas a partir do exame desse material;
- que as informações obtidas da análise do material forense podem ser colocadas em um banco de dados de DNA; e, nesse caso,
- a finalidade da análise é que as informações sejam colocadas em um banco de dados, podendo ser usadas somente com esse fim.

Se o consentimento for retirado, o material forense coletado deve ser destruído e as informações obtidas da análise apagadas assim que possível.

PRINCÍPIO 4

Os procedimentos forenses devem ser realizados por uma pessoa devidamente qualificada.

A legislação nacional normalmente identifica as categorias de pessoas autorizadas para realizar análises forenses. A *Lei Modelo de Análises Forenses* australiana estabelece que as amostras de sangue devem ser obtidas por um médico ou enfermeiro, as radiografias dentais por um médico ou dentista e as amostras de saliva por um médico, enfermeiro, dentista ou uma pessoa qualificada conforme disposto pelo regulamento (por exemplo, um policial).

Em determinados casos, prevê-se também o envolvimento do médico ou dentista do indivíduo em um exame de sexologia forense que envolva um suspeito em uma investigação criminal ou um condenado.

PRINCÍPIO 5

Os dados de DNA coletados para a identificação de pessoas desaparecidas ou restos mortais só podem ser utilizados e divulgados com essa finalidade específica.

Em conformidade com o princípio da especificação da finalidade, os dados pessoais só podem ser coletados, utilizados ou divulgados com um objetivo específico. O mesmo princípio deve se aplicar ao uso de perfis de DNA. Os perfis analisados para fins de identificação só devem ser usados com essa finalidade (ou em investigações criminais e processos civis subsequentes, quando não houver certeza sobre a identidade da pessoa falecida). Devem-se proibir outros usos das informações derivadas da análise de DNA – por exemplo, a tentativa de determinar a etnia ou o estado de saúde da pessoa depois que esta foi identificada, ou a utilização dos dados de DNA para pesquisa científica.

Familiares de pessoas desaparecidas fornecem amostras de DNA para a identificação dos restos mortais de seus entes queridos.



Na legislação nacional esse princípio é implementado de duas maneiras. Em alguns países (tais como França e alguns estados dos Estados Unidos), as análises de DNA se restringem ao DNA não codificante, salvo para determinar o gênero. Esse requisito foi especialmente importante para a *Comissão Nacional de Informática e Liberdades* da França. Outra abordagem consiste em proibir a obtenção de informações de análises de DNA que não sejam as necessárias para fins de identificação. O projeto de lei suíço sobre o uso de perfis de DNA proíbe derivar (ou divulgar) informações de saúde ou outras características pessoais (exceto gênero) das análises de DNA, a menos que isso seja necessário para identificar alguém.

O princípio da especificação da finalidade também é reconhecido na *Recomendação N.º R (92) 1* do Conselho da Europa sobre o uso de análises de DNA no âmbito do sistema de justiça penal. A recomendação, no entanto, não restringe a análise à parte não codificante do DNA. Os especialistas consideraram que isso “limitaria desnecessariamente os países que permitiam o uso do DNA codificante”.²⁵ A Resolução do Conselho da União Europeia de 9 de junho de 1997 relativa ao intercâmbio de resultados de análises de DNA, afirma no seu preâmbulo que “o intercâmbio de resultados de análises de DNA para efeitos de investigação criminal se deve limitar ao intercâmbio de dados da parte não portadora de códigos da molécula de DNA”.

PRINCÍPIO 6

Amostras e perfis de DNA devem ser destruídos/apagados quando as pessoas desaparecidas tiverem sido identificadas, salvo se necessários para fins relacionados.

Algumas legislações nacionais não preveem a destruição das amostras ou a eliminação de informações de DNA. De acordo com as normas canadenses, se uma pessoa for condenada por um delito reconhecido pela lei, as informações podem ser mantidas indefinidamente, a menos que a condenação seja revogada. Geralmente, no entanto, se o indivíduo receber uma absolvição absoluta ou condicional (uma punição menos grave que uma sentença) ou ainda se o indivíduo for uma criança ou adolescente, o acesso às informações deverá ser negado permanentemente e as amostras, destruídas após um período de retenção definido. A legislação do Reino Unido estabelece que as amostras devem ser destruídas quando o suspeito é declarado inocente ou as acusações são retiradas, mas os perfis de DNA podem ser mantidos. Outras leis preveem um período de tempo durante o qual as amostras ou as informações devem ser mantidas. A legislação holandesa determina que os dados sobre pessoas que são erroneamente consideradas suspeitas devem ser removidos, mas outros dados podem ser mantidos por até 30 anos. As informações da cena do crime são mantidas por 18 anos. No caso de testes de DNA em massa para a investigação de crimes graves, a prática parece ser a de destruir as amostras voluntárias após a resolução do crime.

PRINCÍPIO 7

As análises de DNA só devem ser realizadas por laboratórios certificados ou credenciados.

A *Recomendação N.º R (92) 1* do Conselho da Europa enumera uma série de critérios a serem seguidos por laboratórios ou instituições credenciadas para a realização de exames de DNA, incluindo:

²⁵ Tradução livre do CICV.

- elevado conhecimento e competência profissional, juntamente com procedimentos adequados de controle de qualidade;
- integridade científica;
- segurança apropriada das instalações e das substâncias sob investigação;
- garantias adequadas para assegurar uma absoluta confidencialidade com relação à identidade da pessoa a qual a análise de DNA se refere;
- garantias de que serão seguidas as condições estipuladas pela *Recomendação*.

A norma também recomenda a implantação de procedimentos para a supervisão regular dos laboratórios credenciados.

A maioria das legislações nacionais impõe condições sobre os laboratórios credenciados para que realizem testes de DNA garantindo a segurança e a confidencialidade. Os procedimentos para a supervisão regular foram estabelecidos segundo a lei francesa e de diversos estados dos Estados Unidos (por exemplo, Nova York e Massachusetts).

PRINCÍPIO 8

As amostras, os perfis e os registros de DNA devem ser adequadamente protegidos contra o acesso e o uso não autorizados.

As salvaguardas adequadas devem proteger as amostras e informações de DNA contra perda ou roubo, acesso não autorizado, divulgação, cópia, uso ou modificação, independentemente do formato em que sejam mantidas. Essa proteção pode incluir tanto a segurança física (por exemplo, restrição do acesso aos estabelecimentos que armazenam os registros ou amostras) como medidas de segurança técnica (criptografia, firewalls, entre outras). As pessoas e os funcionários que tratem ou processarem os dados devem assinar um termo de confidencialidade.

O projeto de lei suíço sobre a utilização de perfis de DNA estabelece, por exemplo, que tais perfis devem ser mantidos separados de outros dados pessoais e acessíveis somente por meio de um código. A maioria das outras legislações domésticas não têm esse requisito específico, mas exige um nível de segurança condizente com a sensibilidade das informações que os testes de DNA possam produzir.

PRINCÍPIO 9

Os perfis ou amostras de DNA só devem ser divulgados, transferidos ou comparados no contexto da cooperação internacional para fins de identificação e somente com o consentimento das pessoas em questão, salvo em determinados casos. As amostras de DNA não devem ser transferidas, exceto quando a análise for realizada no exterior.

Antes da transferência de dados sensíveis para o exterior, as autoridades que os transferem devem especificar quais usos e divulgações são permitidas a quem as receber. As autoridades também devem obter garantias válidas do destinatário de que tais informações só serão utilizadas e divulgadas para esses objetivos, com a devida aplicação de princípios da informação justa (por exemplo, medidas de segurança e períodos de retenção). Só então os dados deverão ser transferidos.

Devem-se adotar garantias similares caso seja necessária a transferência de amostras de DNA (por exemplo, para análises genéticas a serem realizadas em um laboratório no exterior). Se as informações de DNA estiverem disponíveis de outras formas, não é adequado transferir as amostras em si, já que isso aumentaria o risco de que testes adicionais sejam realizados sobre o DNA para fins não autorizados pelo país que o transfere.

MISSÃO

O Comitê Internacional da Cruz Vermelha (CICV) é uma organização imparcial, neutra e independente, cuja missão exclusivamente humanitária é proteger a vida e a dignidade das vítimas de conflitos armados e outras situações de violência, assim como prestar-lhes assistência. O CICV também se esforça para evitar o sofrimento por meio da promoção e do fortalecimento do direito e dos princípios humanitários universais. Fundado em 1863, o CICV deu origem às Convenções de Genebra e ao Movimento Internacional da Cruz Vermelha e do Crescente Vermelho. Dirige e coordena as atividades internacionais que o Movimento conduz em conflitos armados e outras situações de violência.



CICV