Le pouvoir de l'humanité
XXXIVe Conférence internationale
de la Croix-Rouge et du Croissant-Rouge
28-31 octobre 2024, Genève

Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles

RAPPORT INTÉRIMAIRE

Septembre 2024

FR
34IC/24/10.4
Original : anglais
Pour information

Document établi par
le Comité international de la Croix-Rouge en consultation avec le Groupe chargé de l'application du Code de conduite relatif à la protection des données à caractère personnel pour les activités de RLF

RAPPORT INTÉRIMAIRE

Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles

RÉSUMÉ

L'impact des disparitions et des séparations familiales sur les individus, les familles et les communautés constitue l'une des plus graves tragédies humanitaires à long terme. Les services de rétablissement des liens familiaux (RLF) proposés par le Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) englobent toute une gamme d'activités visant, entre autres, à prévenir les séparations familiales, à rétablir et maintenir le contact entre les membres de familles dispersées, à rechercher des informations et des réponses pour les proches de personnes disparues, ainsi qu'à faciliter le regroupement des familles, lorsque cela est possible.

Des activités de RLF efficaces et efficientes[1] nécessitent de traiter en permanence des données personnelles et notamment de les transférer d'un pays à l'autre. Sans transmission et sans recoupement des données, il serait tout simplement impossible de fournir des services de cette nature. Le développement rapide des technologies numériques et de l'utilisation des données permet désormais de collecter plus vite et plus facilement de gros volumes de données personnelles. Le Mouvement reconnaît le potentiel énorme que ces évolutions représentent pour ses services de RLF, mais il est aussi conscient des risques qu'elles impliquent et donc de l'importance d'élaborer et d'appliquer des normes appropriées en matière de protection des données.

En 2015, le Mouvement a adopté le *Code de conduite relatif à la protection des données à caractère personnel pour les activités de RLF* (Code de conduite). Applicable à toutes les composantes du Mouvement, il s'aligne sur les normes les plus strictes en matière de protection des données. En harmonisant les bonnes pratiques, il favorise une gestion adéquate des données au sein du Réseau des liens familiaux[2] et garantit des échanges de données sécurisés à l'intérieur du Mouvement et avec d'autres acteurs. De plus, le Code de conduite s'est avéré particulièrement utile pour faire face à la violation de données dont le Comité international de la Croix-Rouge (CICR) a fait l'objet en 2022. L'Agence centrale de recherches, en coopération avec le Groupe chargé de l'application du Code de conduite relatif à la protection des données à caractère personnel pour les activités de RLF (Groupe chargé de l'application du Code de conduite)[3], a soutenu le Réseau des liens familiaux dans ses efforts pour renforcer sa conformité avec les dispositions dudit Code de conduite. À cette fin, un plan d'action s'appuyant sur trois piliers a été mis en place :

- l'élaboration d'orientations et la promotion des bonnes pratiques,
- la formation,
- l'établissement de rapports.

[1] Le rétablissement des liens familiaux, ou RLF, est le terme générique utilisé par le Mouvement pour désigner l'ensemble des activités visant à prévenir les séparations et les disparitions, à élucider le sort des personnes portées disparues et à les localiser, à rétablir et maintenir le contact entre les membres de familles dispersées et à faciliter leur regroupement.
[2] Le Réseau des liens familiaux se compose de l'Agence centrale de recherches, des unités RLF au sein des délégations du Comité international de la Croix-Rouge (CICR), ainsi que des services de RLF/de recherches des Sociétés nationales de la Croix-Rouge et du Croissant-Rouge.
[3] Ce groupe fournit des orientations et un soutien au Réseau des liens familiaux sur tous les sujets liés à la mise en œuvre et à la promotion du Code de conduite aux échelons régional et mondial.

Selon les principes internationalement reconnus en matière de protection des données, tout traitement de données personnelles doit reposer sur une base légitime. Conformément aux traités de droit international humanitaire (DIH), aux Statuts du Mouvement et aux résolutions pertinentes de la Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale), le Mouvement a pour mandat de porter assistance aux victimes des crises humanitaires. Il en découle que le traitement des données personnelles à des fins de RLF est justifié par des motifs d'intérêt public.

Malgré cette reconnaissance, nous observons encore que de nombreuses Sociétés nationales de la Croix-Rouge et du Croissant-Rouge (Sociétés nationales) ne sont pas autorisées à s'appuyer sur cette base légale, ce qui revient à nier le fait que les opérations de traitement des données effectuées par le Mouvement visent des fins exclusivement humanitaires. Par conséquent, celui-ci rappelle aux États l'importance de fournir aux Sociétés nationales des bases juridiques appropriées et de s'abstenir de demander un accès aux données recueillies dans le cadre des activités de RLF s'ils ont l'intention de les utiliser à d'autres fins, autres qu'humanitaires. Cela est primordial pour réduire les risques considérables pour la dignité et la sécurité des individus touchés par des urgences humanitaires, dont les données personnelles revêtent un caractère particulièrement sensible.

De plus, la cyberattaque dirigée contre les serveurs du CICR en 2022 a mis en lumière les risques que les cyberopérations et les violations de données font peser sur les organisations humanitaires et les personnes auxquelles elles s'efforcent de venir en aide. Le Mouvement a traité ce sujet dans la résolution 12 du Conseil des Délégués de 2022, intitulée « La protection des données humanitaires »[4], qui visait à accorder aux données personnelles collectées à des fins humanitaires (données humanitaires), et aux infrastructures numériques qui les hébergent, une protection spéciale contre les cyberopérations, les intrusions et les utilisations abusives.

En outre, nous insistons auprès des États sur la nécessité de reconnaître que les activités de RLF impliquent de fréquents échanges transfrontaliers de données personnelles pour être efficaces. Ces échanges devraient donc être aussi peu limités que possible, tout en demeurant conformes aux obligations strictes en matière de protection des données. Les normes exigeantes du Code de conduite devraient contribuer à renforcer la confiance des individus et des autorités de réglementation à l'égard des activités menées par le Mouvement, et fournissent des garanties aux composantes du Mouvement qui sont amenées à se transférer mutuellement des données personnelles.

1) INTRODUCTION

Le Réseau des liens familiaux et les services de RLF qu'il fournit jouent de longue date un rôle central en aidant les autorités à honorer leurs obligations dans ce domaine. Le DIH, qui s'applique dans les situations de conflit armé, contient de fait des règles portant sur le respect de la vie familiale, le maintien ou le rétablissement des liens familiaux et la nécessité de faire la lumière sur le sort des personnes portées disparues par suite d'un conflit armé[5]. D'autres instruments internationaux établissent également des droits liés au respect de la vie et de l'unité familiales, ainsi qu'au regroupement des familles[6].

[4] Résolution 12 du Conseil des Délégués de 2022, intitulée « La protection des données humanitaires », disponible sur : https://rcrcconference.org/app/uploads/2022/06/CD22-R12-Safeguarding-Humanitarian-Data_23-June-2022_FINAL_FR.pdf.

[5] Il s'agit notamment de l'obligation découlant des Conventions de Genève de 1949 – et développée dans le Protocole additionnel I de 1977 – consistant à faciliter les recherches qu'entreprennent les membres des familles dispersées par suite d'un conflit armé, et à prendre toutes les mesures possibles pour rétablir les liens familiaux et faciliter le regroupement de ces familles. Les États parties aux Conventions de Genève ont aussi l'obligation de permettre à toute personne se trouvant sur leur territoire de donner aux membres de sa famille, où qu'ils se trouvent, des nouvelles de caractère strictement familial et d'en recevoir. En outre, le Protocole additionnel II dispose que les enfants recevront les soins et l'aide dont ils ont besoin et, en particulier, que toutes les mesures appropriées seront prises pour faciliter le regroupement des familles momentanément séparées.

[6] Voir, par exemple, la Déclaration universelle des droits de l'homme, art. 16 (1948) ; le Pacte international relatif aux droits économiques, sociaux et culturels, art. 10 (1966) ; le Pacte international relatif aux droits civils et politiques, art. 23 (1966) ; la Convention relative aux droits de l'enfant, art. 9, 10, 20 et 22 (1989) ; et la Convention internationale pour la protection de toutes les personnes contre les disparitions forcées, art. 17, 24 et 25 (2006).

Les conflits armés, les autres situations de violence et les catastrophes engendrent toujours autant de besoins en RLF. Cependant, ces 15 dernières années, le Mouvement a également intensifié son action afin de répondre aux besoins, souvent négligés, des proches de personnes disparues et des familles séparées dans le contexte de la migration. Faute de mécanismes efficaces et de coopération entre les États pour élucider le sort des migrants disparus et les localiser, les familles de ces derniers sont abandonnées à leurs questions sans réponse.

Le nombre croissant de personnes qui sollicitent des services de RLF auprès du Mouvement témoigne des attentes quant à un Réseau des liens familiaux solide et mondial. Il signifie également que le Mouvement est amené à recueillir des volumes considérables de données personnelles et ce, dans des contextes parfois fragiles et instables. Conformément aux traités de droit international humanitaire (DIH), aux Statuts du Mouvement et aux résolutions pertinentes de la Conférence internationale, le Mouvement a pour mandat de porter assistance aux victimes des crises humanitaires. Il en découle que le traitement des données personnelles à des fins de RLF est justifié par des motifs d'intérêt public.

2) CONTEXTE

La Conférence internationale a déjà affirmé l'importance du RLF à de multiples reprises. Ainsi, la XXIV^e^ Conférence invitait les Sociétés nationales à mener des activités de recherches et de regroupement familial, et priait les gouvernements de faciliter l'action du Mouvement et de lui apporter tout le soutien nécessaire. La XXVI^e^ Conférence demandait aux États d'accorder aux Sociétés nationales l'accès aux données pertinentes et de faciliter leurs activités de recherches et de regroupement familial en période de conflit armé. Quant à la XXVIII^e^ Conférence, elle définissait une série d'objectifs en lien avec les personnes portées disparues lors de conflits armés ou d'autres situations de violence. Ces objectifs consistaient notamment à prévenir les disparitions, élucider le sort des personnes disparues, gérer les informations et traiter les dossiers relatifs aux personnes disparues. Dans sa résolution 4, la XXXIII^e^ Conférence internationale a rappelé que la protection des données personnelles est étroitement liée au respect de la vie privée, tout en soulignant que leur traitement fait partie intégrante des services de RLF et qu'il est essentiel à l'accomplissement du mandat des composantes du Mouvement.

Le Mouvement a fait preuve de son engagement en faveur d'une gestion et d'un traitement responsables des données en élaborant le Code de conduite, qui a été le premier document de cet ordre à traiter la question au sein du Mouvement. Il énonce les principes, procédures et engagements minimaux que les composantes du Mouvement doivent respecter lorsqu'elles traitent des données dans le cadre du Réseau des liens familiaux. Un groupe de travail[7] a été spécialement créé pour appuyer l'application du Code de conduite au niveau mondial. À travers la réalisation de notre Stratégie de RLF 2008-2018, la mise en œuvre de la Stratégie de RLF 2020-2025 et sa prolongation prévue jusqu'en 2030, ainsi que l'application du Code de conduite, nous réaffirmons notre engagement en faveur de la protection des données, condition indispensable au traitement des données personnelles.

3) PROGRÈS RÉALISÉS

Pour assurer le bon fonctionnement du Réseau des liens familiaux, il est essentiel que les membres de la Conférence internationale réaffirment auprès des États le rôle spécifique du Mouvement et ses capacités en matière de RLF, ainsi que le soutien qu'il peut leur apporter en vue de les aider à honorer leurs obligations et engagements envers les familles dispersées, les personnes portées disparues et leurs familles, notamment envers les migrants portés disparus. Les composantes du Mouvement doivent s'attacher à poursuivre leur coopération avec les autorités et les autres parties prenantes clés, en faisant preuve de circonspection et

[7] Le Groupe chargé de l'application du Code de conduite relatif à la protection des données à caractère personnel pour les activités de RLF.

en mettant en place des procédures transparentes permettant de protéger efficacement les personnes qui font appel à nos services de RLF, ainsi que leurs données sensibles.

Les services de RLF, plus que tout autre service proposé par le Mouvement, reposent sur le traitement de données personnelles dans la mesure où ils exigent de pouvoir transmettre et recouper ce type de données. Il est crucial que les États reconnaissent davantage cette particularité et la nécessité de préserver sa finalité humanitaire.

A) INTÉGRER L'ACTION HUMANITAIRE DANS LES LÉGISLATIONS SUR LA PROTECTION DES DONNÉES

Depuis que la résolution a été adoptée, des lois et des réglementations sur la protection des données ont été mises en place ou actualisées dans de nombreux pays, preuve que ceux-ci sont de plus en plus conscients de l'importance d'établir des principes et des normes pour réglementer le traitement des données personnelles. Cependant, ces textes législatifs ne tiennent pas toujours compte de l'incidence de leurs dispositions sur le travail des acteurs humanitaires, notamment de ceux qui sont pleinement soumis à la législation nationale. Ce constat découle de l'analyse de deux éléments clés :

i. La nécessité d'une base juridique appropriée pour que les Sociétés nationales puissent accomplir leur mandat humanitaire

En adoptant la résolution, les États ont reconnu qu'il est difficile, voire souvent impossible, d'obtenir le consentement des personnes bénéficiant d'un service de RLF, du fait de leur vulnérabilité et de la nature des opérations humanitaires. La résolution souligne par ailleurs qu'il serait possible de fonder le traitement des données personnelles à des fins de RLF sur d'autres bases valables, notamment des motifs importants d'intérêt public, des intérêts vitaux et le respect d'une obligation légale. Il est particulièrement légitime d'invoquer des motifs importants d'intérêt public dans le cadre des activités de RLF, dans la mesure où le traitement des données personnelles relève de notre mandat humanitaire et qu'il est nécessaire pour accomplir les tâches énoncées dans les Statuts du Mouvement. Pourtant, un nombre important de Sociétés nationales ne peuvent pas faire valoir l'intérêt public ou d'autres bases légales valables dans leur cadre juridique national, ce qui ne leur laisse pas d'autre choix que de s'appuyer sur le consentement.

Les États sont encouragés à poursuivre leurs efforts en vue d'établir un lien direct entre l'action humanitaire, notamment le RLF, et le traitement des données personnelles fondé sur d'autres bases juridiques légitimes, dont les motifs importants d'intérêt public. Dans certains cas, la législation nationale relative à la protection des données, qu'elle soit entrée en vigueur avant ou après l'adoption de la résolution[8] objet du présent rapport, ne retient pas l'intérêt public comme l'une des bases juridiques appropriées. Dans d'autres cas, il a été jugé que l'intérêt public ne constituait pas un motif légitime pour le traitement de données sensibles, pourtant reconnu comme un aspect essentiel des activités de RLF.

ii. Le transfert international de données personnelles

La fourniture de services de RLF nécessite un échange continu de très nombreuses informations au sein des Sociétés nationales et des délégations du CICR, mais aussi entre elles. Des données doivent donc être transférées d'un pays à l'autre, principalement *via* des plateformes numériques sécurisées mises à disposition par l'Agence centrale de recherches,

[8] Résolution 4 de la XXXIII[e] Conférence internationale, disponible sur : https://rcrcconference.org/app/uploads/2019/12/IC33-R4-RFL-Data-protection_ADOPTED-clean_fr.pdf.

telles que *Secure File Exchange* (SFE)[9] et *Family Links Answers* (FL ANSWERS)[10]. Cependant, il arrive encore trop souvent que les législations nationales sur la protection des données imposent des restrictions au transfert de données personnelles à des entités situées à l'étranger et ce, sans prévoir d'exemptions pour les organisations humanitaires, quand bien même il a été reconnu que le transfert desdites données au sein du Mouvement devrait être aussi peu restreint que possible. Dans certains cas, il peut être nécessaire de solliciter une autorisation spéciale auprès des autorités de contrôle nationales. Dans d'autres, ces autorités exigent une évaluation du cadre juridique du pays de destination, mais sans fournir les orientations ou les outils nécessaires à cette fin.

Il est essentiel que le Mouvement et les États continuent de mener des efforts coordonnés pour limiter l'impact des législations nationales relatives à la protection des données sur les activités humanitaires.

B) PROTÉGER LES ACTEURS HUMANITAIRES POUR PROTÉGER LES DONNÉES

Dans sa résolution, la Conférence internationale a reconnu que la protection des données est essentielle à l'accomplissement du mandat humanitaire du Mouvement. Cependant, celui-ci peine encore à accéder à certaines informations ou à voir ses données protégées, malgré le soutien fourni par les États et les progrès qu'ils ont accomplis dans ce domaine. Il a été constaté que certains États hésitent à ouvrir leurs bases de données au Mouvement, alors que celles-ci pourraient lui être d'une aide précieuse pour ses activités de RLF. Ils invoquent des problèmes de protection des données qui, après analyse, peuvent se révéler insuffisamment fondés. Par conséquent, cette position fait obstacle à la poursuite des objectifs humanitaires du Mouvement, lesquels devraient, en soi, constituer une base légitime pour le traitement des données. Dans d'autres cas, il a été demandé aux Sociétés nationales de divulguer des données personnelles à des fins incompatibles avec leur mission humanitaire ou contraires à la résolution. De telles pratiques compromettent l'efficacité des services de RLF et risquent de nous faire perdre la confiance des personnes affectées, dont nous avons besoin pour accomplir notre mission. En outre, elles vont à l'encontre du principe consistant à « ne pas nuire ».

À ces difficultés s'ajoutent les menaces découlant des cyberattaques et des incidents de sécurité. La cyberopération dirigée en 2022 contre des serveurs hébergeant des données du CICR et de plus de 60 Sociétés nationales a mis en lumière les risques que les cyberopérations et les violations de données représentent pour les organisations humanitaires[11] et les personnes affectées qui bénéficient de leurs services, dans la mesure où les données de plus de 500 000 personnes ont été touchées.

À la suite de cette attaque, les serveurs ont dû être mis hors ligne et les systèmes reconstruits. L'Agence centrale de recherches a coordonné les mesures prises par le Mouvement en réaction à la cyberopération. Grâce au précieux soutien apporté par des informaticiens et des juristes spécialisés de l'ensemble du Mouvement, les délégations du CICR et les Sociétés nationales concernées ont procédé individuellement à des analyses pour identifier les données et les personnes touchées par la violation. Elles ont également effectué une évaluation des risques pour déterminer s'il convenait de prévenir non seulement les autorités, mais aussi les personnes affectées, ainsi que pour définir des mesures d'atténuation destinées à soutenir ces dernières. Selon la sensibilité du contexte, il a aussi été crucial de choisir des moyens appropriés pour avertir ces personnes. Le Mouvement a ainsi recouru à différentes solutions adaptées à chaque situation : annonces publiques, appels téléphoniques, rencontres en

[9] SFE est une plateforme en ligne permettant d'échanger des documents en lien avec les activités de protection au sein des Sociétés nationales et du CICR, et entre ceux-ci. Dans le cas du Réseau des liens familiaux, elle sert à échanger des documents électroniques ayant trait aux dossiers de RLF en cours qui contiennent des données personnelles.
[10] FL ANSWERS est une application Web destinée à faciliter les activités de RLF des Sociétés nationales. Il permet de renforcer la gestion et le suivi des dossiers de RLF et comporte un module spécialement destiné aux Sociétés nationales qui mènent des activités dans les lieux de privation de liberté.
[11] Pour de plus amples informations, voir : https://www.icrc.org/fr/document/cyberattaque-cicr-ce-que-nous-savons.

personne, lettres et courriels. La cyberattaque a été lourde de conséquences, au premier rang desquelles figurent une perte de confiance dans le Mouvement et un ralentissement considérable des services de RLF dans le monde entier. Les effets de la violation de données se sont ressentis pendant des mois après sa découverte.

Fort heureusement, le Code de conduite prévoyait les principes et les procédures à appliquer en cas de violation de données et a donc joué un rôle essentiel pour surmonter la crise. Le cadre qu'il fournit s'est révélé d'une grande aide pour déterminer si l'incident répondait à la définition d'une violation de données, ainsi que pour coordonner l'analyse des risques et l'instauration d'un dialogue avec les usagers du système et les personnes concernées, lorsqu'il a été jugé que l'incident était susceptible de porter atteinte à leurs droits et leurs libertés[12].

Les perturbations engendrées par les attaques de cette nature mettent en péril l'action humanitaire. Il est par conséquent essentiel de réitérer le message lancé dans la résolution du Conseil des Délégués sur « la protection des données humanitaires » et d'appeler de nouveau les États à respecter et protéger les organisations humanitaires – y compris les Sociétés nationales, leurs volontaires et leur personnel, leurs données et leurs actifs[13] – en reconnaissant dans leurs stratégies nationales de cybersécurité le rôle vital que ces organisations jouent en tant qu'infrastructures indispensables et en adoptant des mesures législatives destinées à permettre une réponse immédiate aux menaces externes pesant sur leurs données.

C) EFFORTS DU MOUVEMENT POUR RENFORCER LE RESPECT DES REGLES RELATIVES A LA PROTECTION DES DONNEES

Depuis que la résolution a été adoptée, le Mouvement s'est attaché à mieux comprendre la protection des données, et notamment le fait qu'elle concerne l'ensemble des activités de RLF. Le Groupe de mise en œuvre de la Stratégie de RLF 2020-2025 (Groupe de mise en œuvre), qui est chargé de veiller à l'application de la résolution, a joué un rôle essentiel à cet égard. Avec le soutien du Groupe chargé de l'application du Code de conduite, au sein duquel sont représentés le CICR, des Sociétés nationales issues de différentes régions et la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Fédération internationale), ce groupe apporte son appui au Mouvement sur toutes les questions relatives à la mise en œuvre et à la promotion du Code de conduite aux niveaux national, régional et mondial.

Dans le cadre de ces efforts, le Groupe chargé de l'application du Code de conduite a élaboré les indicateurs clés de suivi utilisés dans le cadre de suivi et d'évaluation de la Stratégie de RLF, afin de mesurer annuellement la conformité de chaque composante du Mouvement vis-à-vis de la protection des données. Les composantes peuvent en outre utiliser ces indicateurs pour élaborer leur propre stratégie en matière de protection des données.

La dernière enquête d'auto-évaluation lancée par l'Agence centrale de recherches en 2024, dans le cadre de laquelle toutes les composantes ont été invitées à mesurer elles-mêmes leur conformité avec les règles relatives à la protection des données, a fait ressortir une dynamique globalement positive au sein du Mouvement : d'après leur résultat général, le pourcentage de composantes pleinement conformes est passé de 1,3% à 5%, tandis que le taux de celles affichant une conformité moyenne a grimpé de 18% à 21%. En revanche, 50% du Mouvement déclare encore avoir un faible niveau de conformité et 2% ne pas être en conformité du tout[14].

[12] Paragraphe 2.3.8 du Code de Conduite.
[13] Paragraphe 13 de la résolution 12 relative à « la protection des données humanitaires ».
[14] Ces taux ont été obtenus à partir des réponses aux questions sur les indicateurs clés de suivi. Il existe neuf indicateurs de ce type pour les Sociétés nationales et six pour les délégations du CICR. Parmi ces indicateurs, six sont considérés essentiels pour les Sociétés nationales, contre quatre pour le CICR. Pour être pleinement conforme, une Société nationale ou une délégation du CICR doit s'évaluer positivement au regard de l'ensemble des indicateurs clés de suivi ; pour une conformité moyenne, elles doivent répondre « oui » ou « en partie » aux questions sur les indicateurs essentiels ; pour un faible niveau de

Le Groupe chargé de l'application du Code de conduite a mis au point un plan d'action destiné à utiliser cet instrument pour renforcer la protection des personnes affectées moyennant une meilleure protection de leurs données personnelles. À cette fin, il a identifié trois piliers : l'élaboration d'orientations, la formation et l'établissement de rapports. Un juriste spécialiste de la protection des données a été recruté et confirmé à son poste afin de soutenir les Sociétés nationales dans leurs efforts pour améliorer leur conformité avec les règles dans ce domaine.

Ce groupe a également élaboré un modèle concis et compréhensible de notice d'information pour faciliter l'application du principe de transparence envers les personnes affectées, ainsi qu'un formulaire-type permettant à ces dernières d'exercer leur droit d'opposition.

Le Groupe chargé de l'application du Code de conduite a en outre soutenu les efforts déployés pour mieux respecter les règles relatives à la protection des données, en mettant à la disposition du Mouvement :

- un modèle pour aider à la création d'une politique d'archivage,
- une liste de contrôle pour faciliter l'analyse du cadre juridique national relatif à la protection des données,
- un mécanisme d'échange des bonnes pratiques relatives à l'application du Code de conduite,
- des orientations sur la conservation et la suppression des données,
- un modèle d'accord sur le partage des données à l'usage des Sociétés nationales amenées à transmettre des données personnelles à des entités extérieures au Mouvement.

Les Sociétés nationales sont de plus en plus nombreuses à avoir désigné une personne référente pour la protection des données de RLF. Cette personne est chargée de s'assurer que la Société nationale tient compte de la protection des données dans ses opérations. En outre, plusieurs membres du Mouvement ont lancé des initiatives intéressantes pour sensibiliser et former leur personnel et leurs volontaires à cette problématique. Le CICR a organisé une série de webinaires à l'intention de ses délégations et des Sociétés nationales, dans le but de leur expliquer la méthodologie et le contenu des documents-types relatifs à la protection des données, à la lumière des exigences du Code de conduite. Plusieurs séances de formation sur la protection des données de RLF ont également été menées en ligne et en face à face dans divers pays.

De plus, le CICR s'est associé à l'Université de Maastricht pour mettre au point et lancer un programme de formation et de certification destiné aux responsables de la protection des données dans l'action humanitaire[15]. Depuis 2021, 13 sessions ont été organisées dans différentes régions du monde. En mai 2024, 259 membres du personnel de Sociétés nationales et 61 membres du personnel du CICR avaient bénéficié des systèmes de parrainage mis en place par le CICR, avec le soutien du ministère des Affaires étrangères et européennes du Luxembourg.

Pour renforcer la sécurité des données, l'Agence centrale de recherches a mis à la disposition du Mouvement une plateforme d'échange sécurisé de documents ainsi qu'un outil de gestion sécurisée de dossiers, qui est désormais utilisé par plus de 70 Sociétés nationales.

Enfin, le CICR collabore avec la Fédération internationale afin d'aider des Sociétés nationales de plusieurs régions à se doter d'adresses électroniques institutionnelles. Cependant, dans les contextes confrontés à une pénurie de moyens techniques et logistiques, de même que

conformité, elles doivent s'estimer en conformité totale ou partielle avec moins de six indicateurs essentiels ; une conformité nulle correspond à une réponse négative pour l'ensemble des neufs indicateurs clés de suivi.

[15] Programme de certification des responsables de la protection des données dans l'action humanitaire, Université de Maastricht : https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-humanitarian-action-certification (en anglais).

dans les situations d'urgence où l'on peut craindre que les personnes affectées ne soient exposées à des risques plus élevés en cas de perte, d'utilisation inappropriée ou de consultation non autorisée de leurs données, les États, le secteur privé et le Mouvement devront fournir un soutien accru pour permettre aux Sociétés nationales d'accomplir de réels progrès en matière de numérisation et de sécurité des données.

4) INCIDENCES EN TERMES DE RESSOURCES

Pour fonctionner de manière adéquate et efficace, le Réseau des liens familiaux doit pouvoir compter sur les ressources suivantes : une expertise technique et un leadership au niveau mondial, régional et national, du personnel et des volontaires dévoués et bien formés, un accès aux technologies numériques, la capacité de répondre aux situations d'urgence et d'intensifier son action en cas de besoin, et une flexibilité suffisante pour offrir le meilleur service possible par les moyens les plus appropriés. Des ressources financières seront nécessaires pour atteindre les objectifs de la Stratégie de RLF 2020-2025 et de sa probable prolongation jusqu'en 2030. Nous continuerons de solliciter le soutien des gouvernements.

5) MISE EN ŒUVRE ET SUIVI

Le Groupe de mise en œuvre, avec l'appui technique du Groupe chargé de l'application du Code de conduite, continuera de diriger la mise en œuvre de la résolution. Conformément à la Stratégie de RLF, le Mouvement poursuivra ses efforts pour appliquer les règles relatives à la protection des données et fera rapport annuellement sur les progrès accomplis à cet égard. La communication de ces progrès aux membres de la Conférence internationale sera encouragée dans le cadre du dialogue bilatéral que chaque Société nationale entretient avec les autorités compétentes de son pays en vue de promouvoir la coopération. À l'échelon mondial, des rapports intérimaires seront présentés à la Conférence internationale et au Conseil des Délégués.

6) CONCLUSION ET RECOMMANDATIONS

Pour assurer le bon fonctionnement du Réseau des liens familiaux, il est essentiel que les membres de la Conférence internationale réaffirment le rôle particulier que nous jouons en matière de RLF et la coopération que nous entretenons avec les États dans ce domaine, en reconnaissant la nécessité pour le Mouvement de satisfaire ses besoins pour accomplir son mandat humanitaire.

Les États et les composantes du Mouvement doivent s'engager conjointement dans ce processus et le dialogue en cours ; il y va de la légitimité et de la réputation de toutes les composantes du Mouvement en tant qu'institutions fiables visant des objectifs exclusivement humanitaires. Notant que la résolution demeure valable, le CICR recommande de poursuivre les efforts pour la mettre en œuvre et de reconnaître ainsi l'utilité du Réseau des liens familiaux et le soutien qu'il apporte aux familles dispersées et aux proches de personnes disparues dans le monde entier.

Le CICR et le Groupe de mise en œuvre continueront de recommander aux États d'accorder une protection spéciale aux données personnelles traitées dans le cadre des services de RLF contre les demandes ou les utilisations visant des fins autres qu'humanitaires. De plus, nous appelons les États à respecter et protéger le Mouvement dans l'environnement numérique en faisant en sorte que leur législation nationale préserve la confidentialité, l'intégrité et la disponibilité des données personnelles recueillies aux fins de RLF, ainsi qu'à offrir des garanties contre les cyberattaques et les opérations d'information hostiles.

Le CICR et le Groupe de mise en œuvre continueront par ailleurs de recommander aux États d'identifier, dans leur législation nationale sur la protection des données, des bases juridiques appropriées, comme celles relatives aux motifs importants d'intérêt public, aux intérêts vitaux

et au respect d’une obligation légale, de sorte à permettre au Réseau des liens familiaux de traiter les données humanitaires. Nous insistons en outre sur l’importance de prévoir des bases juridiques permettant aux composantes du Mouvement de se transférer sans difficulté des données personnelles d’un pays à l’autre.

L’Agence centrale de recherches reconnaît et promeut le rôle essentiel que joue la protection des données pour protéger la vie, la dignité, l’intégrité et la sécurité des personnes affectées qui bénéficient des services de RLF. Par conséquent, elle continuera de soutenir le Réseau des liens familiaux dans ses efforts pour respecter les règles dans ce domaine.