



Power of humanity

Council of Delegates of the International
Red Cross and Red Crescent Movement

27–28 October 2024, Geneva

La protection des données humanitaires

RAPPORT INTÉRIMAIRE

Septembre 2024

FR

CD/24/19
Original : anglais
Pour information

Document établi par
le Comité international de la Croix-Rouge
et la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge

RAPPORT INTÉRIMAIRE

La protection des données humanitaires

RÉSUMÉ

En 2022, le Conseil des Délégués du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) a adopté une résolution intitulée « [La protection des données humanitaires](#) ». Cette résolution constituait un effort conjoint du Mouvement visant à prendre conscience des menaces que représentent les cyberopérations, en particulier les violations de données, pour le travail des organisations humanitaires, à préconiser l'adoption de mesures juridiques et politiques afin de protéger ces organisations de telles menaces et à harmoniser les mesures que les composantes du Mouvement peuvent et devraient prendre pour empêcher la consultation non autorisée de données humanitaires.

Dans ce rapport intérimaire, le Comité international de la Croix-Rouge (CICR) et la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Fédération internationale) présentent certaines des mesures particulières adoptées par des composantes du Mouvement pour préserver les données humanitaires qui leur sont confiées, rappellent certaines des mesures juridiques et politiques prises par le CICR pour renforcer les cadres relatifs à la protection des données humanitaires, et rendent compte de certains travaux de recherche et d'innovation menés par le CICR et par la Fédération internationale, en particulier sur l'élaboration d'un emblème numérique.

Le rapport conclut que l'adoption de la résolution relative à la protection des données humanitaires a donné un élan pour renforcer les efforts spécifiques en matière de protection des données au sein du Mouvement. Cependant, toutes les composantes de ce dernier doivent continuer de travailler dans un esprit de solidarité et de responsabilité partagée. Dans l'objectif de renforcer l'harmonisation des politiques au sein du Mouvement et avec les États, certains des engagements et des préconisations contenus dans la résolution seront examinés plus en détail pendant la Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale) en octobre 2024.

1) INTRODUCTION

En conséquence de la violation sans précédent dont ont fait l'objet des données personnelles qui avaient été confiées au CICR et à diverses Sociétés nationales de la Croix-Rouge et du Croissant-Rouge (Sociétés nationales) début 2022, le Conseil des Délégués a adopté, en juin de cette même année, une résolution relative à « [La protection des données humanitaires](#) ».

La résolution constituait un effort conjoint du Mouvement visant à prendre conscience des menaces que représentent les cyberopérations, en particulier les violations de données, pour le travail des organisations humanitaires, à préconiser l'adoption de mesures juridiques et politiques afin de protéger ces organisations de telles menaces et à harmoniser les mesures que les composantes du Mouvement peuvent et devraient prendre pour empêcher la consultation non autorisée de données humanitaires.

Les risques que les cyberopérations, et notamment les violations de données, peuvent entraîner pour les organisations humanitaires sont graves. La violation des données à l'encontre du Mouvement survenue en 2022 a concerné en particulier des données personnelles, telles que le nom, la localisation et les informations de contact de personnes portées disparues et de leurs proches, d'enfants séparés de leurs parents ou non accompagnés, de détenus et d'autres personnes bénéficiant de services humanitaires du fait de conflits armés, de catastrophes naturelles ou de migrations. Si elles tombaient entre de

mauvaises mains, les données volées pourraient être utilisées par des États, des groupes non étatiques ou des individus afin de contacter ou de trouver des personnes et de leur nuire, par exemple en vue d'arrêter ou de cibler des opposants politiques, ou de livrer des enfants non accompagnés à la traite d'êtres humains. En outre, les cyberopérations qui corrompent des données humanitaires risquent de perturber les opérations d'organisations humanitaires et d'éroder la confiance dans leur action. La confiance est indispensable à ces opérations, et une violation des données risque de nuire à l'action des équipes humanitaires, en mettant en péril leur capacité à accéder aux personnes ayant besoin d'aide et en compromettant leur sécurité, et au final d'aggraver encore la situation des personnes qui ont besoin d'aide.

Sur les plans juridique et politique, la résolution a réaffirmé l'engagement du Mouvement à mettre en œuvre des règles en matière de protection des données et des mesures de cybersécurité. Elle a souligné la responsabilité des organisations humanitaires s'agissant de prendre des mesures concrètes et efficaces pour garantir la sécurité des données et protéger toutes les données personnelles qui leur sont confiées. Elle a en outre réaffirmé la protection juridique internationale des organisations humanitaires impartiales en vertu du droit international humanitaire (DIH), qui doit être interprété comme les protégeant également contre tout dommage causé par des moyens numériques. Elle a également souligné que lors d'un conflit armé, d'une catastrophe naturelle ou d'autres situations d'urgence, les activités des organisations humanitaires impartiales doivent être respectées et protégées tant en ligne que hors ligne.

En plus de permettre la cohérence du Mouvement sur les questions d'ordre politique, la résolution a également engagé les composantes du Mouvement à être responsables de l'adoption des mesures appropriées, dans les limites de leurs mandats, de leurs capacités et de leurs besoins et contextes opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de sécurité des données. Cela implique, en particulier, que ces composantes mettent en œuvre les normes et les bonnes pratiques pertinentes dans le cadre du traitement des données personnelles en tenant compte du *Manuel sur la protection des données dans l'action humanitaire* et de la législation applicable au niveau national, et aussi qu'elles échangent de bonnes pratiques sur la protection de ces données, en particulier sur la sécurité des données, se soutiennent mutuellement en vue de renforcer leurs capacités, et envisagent la possibilité d'élaborer un code de conduite du Mouvement pour la protection des données.

2) CONTEXTE

Le présent rapport intérimaire rend compte au Conseil des Délégués de 2024 de certains des travaux réalisés par le Mouvement, en particulier par le CICR et la Fédération internationale, en vue de mettre en œuvre les principaux engagements adoptés dans la résolution de 2022 relative à « La protection des données humanitaires ». La résolution s'appuyait sur celle de 2019 intitulée « Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles », adoptée par la XXXIII^e Conférence internationale. La résolution de 2022 a également constitué un tremplin vers la rédaction de la résolution proposée en 2024 et intitulée « Protéger les civils, ainsi que les autres personnes et biens protégés, contre les cyberopérations et les opérations d'information dans les situations de conflit armé ».

3) AVANCEMENT

Afin de rendre compte de certains des progrès réalisés, la section suivante présentera tout d'abord certaines des mesures concrètes adoptées par les composantes du Mouvement en vue de préserver les données humanitaires qui leur sont confiées. Elle abordera ensuite certaines des mesures d'ordre juridique et politique adoptées par le CICR et par d'autres composantes du Mouvement en vue de renforcer les cadres relatifs à la protection des données humanitaires. Enfin, elle rendra compte de certains travaux de recherche et

d'innovation menés par le CICR et par la Fédération internationale, en particulier au sujet d'un emblème numérique.

A) RENFORCER LES CAPACITÉS EN MATIÈRE DE PROTECTION DES DONNÉES AU SEIN DU MOUVEMENT

En vue de renforcer les capacités en matière de protection des données au sein du Mouvement (et de la communauté humanitaire au sens large), le CICR a mis en place deux programmes d'action humanitaire : un avec l'Université de Maastricht, axé sur la formation et la certification des personnes chargées de la protection des données, et un autre avec l'Université de Cambridge, qui implique la réalisation de recherches conjointes au sujet de la transformation numérique et de ses retombées pour l'action humanitaire. À la date d'avril 2024, le programme de formation et de certification élaboré avec l'Université de Maastricht avait été organisé 13 fois sur quatre continents, formant plus de 450 professionnels du secteur humanitaire, dont plus de 250 faisaient partie du personnel d'une Société nationale et bénéficiaient d'une prise en charge complète.

Le CICR soutient également les Sociétés nationales du monde entier dans leurs efforts pour respecter le *Code de conduite relatif à la protection des données à caractère personnel* pour le Réseau des liens familiaux, en élaborant et en contextualisant des outils de protection des données à travers l'ensemble de ce réseau et en aidant les Sociétés nationales à dialoguer avec leurs autorités, en particulier à la suite de la violation des données survenue en 2022. Plusieurs Sociétés nationales ont beaucoup œuvré en matière de protection des données. Par exemple, en 2023, la Croix-Rouge du Zimbabwe a approuvé un accord sur le respect du *Code de conduite relatif à la protection des données*, destiné à être signé par les employés et les volontaires investis dans le rétablissement des liens familiaux (RLF) ; la Croix-Rouge de l'Ouganda s'est vu remettre par l'autorité locale chargée de la protection des données une certification pour la collecte, le traitement et le contrôle des données ; et la Croix-Rouge australienne a élaboré un exercice de simulation sur la protection des données destiné à son personnel et à ses volontaires affectés au RLF. Les composantes du Mouvement ont également travaillé ensemble dans le cadre du groupe d'application du Code de conduite relatif à la protection des données à caractère personnel pour les activités de RLF et ont élaboré, entre autres choses, une politique générique en matière d'archivage et des lignes directrices concernant la suppression destinées aux membres du Réseau des liens familiaux.

La Fédération internationale a poursuivi l'élaboration de ses pratiques internes concernant la protection des données et a continué de travailler avec les Sociétés nationales pour les aider à appliquer les obligations qui leur incombent en la matière. Par exemple, elle a réalisé plusieurs études d'impact avec des Sociétés nationales concernant la protection des données dans le cadre de projets faisant appel à de nouvelles techniques de traitement des données. Elle a également proposé aux Sociétés nationales des sessions de formation sur la protection des données et a travaillé avec plusieurs d'entre elles pour les aider à élaborer et à mettre en œuvre leurs propres politiques et pratiques connexes à ce sujet. Elle a en outre créé des accords sur le partage des données et des déclarations sur la vie privée normalisés, conçus pour permettre le transfert transparent, sûr et légal de données personnelles en situation d'urgence entre la Fédération internationale et les Sociétés nationales. La Fédération internationale continue d'élaborer avec ces dernières des outils logiciels conçus en tenant compte avant tout de la protection des données et du principe « ne pas nuire ».

B) ÉTABLIR UN CADRE POLITIQUE ET JURIDIQUE INTERNATIONAL SOLIDE POUR LA PROTECTION DES DONNÉES HUMANITAIRES

Même une protection des données solide de la part des organisations humanitaires ne suffira pas, cependant, à empêcher les violations de données. En s'appuyant sur la résolution de 2022, et afin d'alerter les États de ces nouvelles menaces et de renouveler le consensus de longue date concernant la protection des organisations humanitaires contre tout préjudice, le

CICR a [soulevé la question](#) dans le cadre du Groupe de travail à composition non limitée de l'Organisation des Nations Unies (ONU) sur la sécurité du numérique et de son utilisation, et a appelé les États à « réaffirmer que les organisations humanitaires, leur personnel et les données humanitaires ne doivent jamais être pris pour cible, que ce soit dans le monde physique ou dans le monde numérique ». En mai 2024, le Conseil de sécurité de l'ONU a adopté la résolution 2730, qui exprime des préoccupations concernant les violations de données qui ciblent des organisations humanitaires.¹

Nous sommes déterminés à poursuivre les efforts permettant de renforcer les cadres politiques et juridiques, ou à ce qu'ils soient mis en place à cette fin. La XXXIV^e Conférence internationale de 2024, lors de laquelle les participants discuteront de la résolution intitulée « Protéger les civils, ainsi que les autres personnes et biens protégés, contre les cyberopérations et les opérations d'information dans les situations de conflit armé », constituera une occasion capitale pour le Mouvement en vue d'atteindre cet objectif. Cette résolution contient des affirmations sur le cadre juridique relatif à la protection et des engagements des composantes du Mouvement et des États sur le plan politique en vue de protéger les données humanitaires.

Les Sociétés nationales ont pris des mesures concrètes pour renforcer les cadres relatifs à la protection des données humanitaires dans leurs pays respectifs. Par exemple, la Croix-Rouge de Belgique négocie des accords avec les autorités concernant la protection des données humanitaires dans leurs activités conjointes ainsi que des exceptions aux exigences de transfert de données lorsque ces transferts entrent en conflit avec la mission humanitaire de la Société nationale et avec son respect des principes fondamentaux du Mouvement. La Croix-Rouge britannique, de son côté, travaille avec le Bureau du commissaire à l'information du Royaume-Uni et lui demande de confirmer qu'elle peut faire appel à des motifs d'intérêt public lorsqu'elle traite des données personnelles liées à la réalisation de ses activités humanitaires.

C) FAIRE PROGRESSER LA RECHERCHE ET L'INNOVATION

Comme cela est souligné dans la résolution de 2022, toutes les composantes du Mouvement doivent s'efforcer d'investir davantage dans la protection des données. Le CICR réfléchit en parallèle à des mesures techniques pour renforcer la protection des organisations humanitaires et de leurs données contre tout préjudice. Par exemple, en 2022, le CICR a ouvert une délégation dédiée au cyberspace, conçue pour servir de banc d'essai sécurisé pour mener des activités de recherche et développement sur des services numériques sûrs au service des communautés touchées.

En outre, en novembre 2022, le CICR a publié, avec la Croix-Rouge australienne, un rapport sur les avantages, les risques et les solutions possibles concernant la numérisation des emblèmes de la croix rouge, du croissant rouge et du cristal rouge ([Digitalizing the red cross, red crescent and red crystal emblems: Benefits, risks, and possible solutions](#)). Le CICR et la Croix-Rouge australienne ont organisé des consultations régionales avec des Sociétés nationales du monde entier en 2023, et ils ont également créé un groupe de travail sur l'emblème numérique en 2024.

Le projet « Emblème numérique », et notamment la dernière solution technique, à savoir le système d'emblème numérique authentifié (ADEM), a également été présenté à des entreprises, dont bon nombre des principaux fournisseurs de services d'informatique en nuage au niveau mondial. À ce jour, le CICR a mené des consultations bilatérales avec plus de 20 États au sujet du projet pour aborder en particulier la façon d'intégrer l'emblème numérique

¹ Le paragraphe pertinent du préambule est le suivant : « *Se déclarant préoccupé* par la multiplication des activités malveillantes liées aux technologies de l'information et des communications, notamment la fuite de données et les opérations d'information qui ciblent les organisations humanitaires, perturbent leurs opérations de secours, sapent la confiance dans les organisations humanitaires et les activités des Nations Unies, et menacent la sûreté et la sécurité de leur personnel, de leurs locaux et de leurs biens et, en définitive, leur accès et leur capacité de mener à bien des activités humanitaires ».

au DIH et la nécessité de soutenir les travaux relatifs à l'emblème numérique pendant la Conférence internationale. Il a en outre organisé une consultation destinée à tous les États pour présenter et examiner la solution technique proposée concernant un emblème numérique, et a invité tous les États à une consultation sur les questions politiques et juridiques au cours du second semestre de 2024.

6) CONCLUSION ET RECOMMANDATIONS

L'adoption de la résolution relative à « La protection des données humanitaires » a offert l'occasion de réfléchir à certains des travaux menés par le Mouvement en matière de cybersécurité et de protection des données et de les consolider, et a donné un élan pour redoubler les efforts déployés dans ce domaine. Afin de renforcer efficacement la protection des données humanitaires dans l'ensemble du Mouvement, toutes ses composantes doivent continuer de travailler dans un esprit de solidarité et de responsabilité partagée. Pour renforcer l'harmonisation sur le plan politique au sein du Mouvement et avec les États, certains des engagements et des préconisations contenus dans la résolution seront examinés plus en détail pendant la XXXIV^e Conférence internationale.