Le pouvoir de l'humanité

Conseil des Délégués du Mouvement international
de la Croix-Rouge et du Croissant-Rouge

22-23 juin 2022, Genève

La protection des données humanitaires

DOCUMENT DE RÉFÉRENCE

Mai 2022

FR

CD/22/16
Original : anglais
Pour information

Document établi par
le Comité international de la Croix-Rouge
avec l'aval de
la Plateforme de haut niveau sur le rétablissement des liens familiaux

RÉSUMÉ

En 2022, la cyberopération à l'encontre de serveurs hébergeant des données détenues par le Comité international de la Croix-Rouge (CICR) et par plus de 60 Sociétés nationales de la Croix-Rouge et du Croissant-Rouge (Sociétés nationales)[1] a mis en lumière les risques que représentent les cyberopérations et les violations de données pour les organisations humanitaires. Depuis plusieurs années, le CICR et d'autres membres du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) avertissent de la nécessité vitale et urgente pour les États et d'autres acteurs de protéger les données humanitaires et l'infrastructure numérique des cyberopérations, intrusions et usages abusifs de données. La récente violation dont ont fait l'objet des données personnelles a malheureusement montré que ce risque n'est que trop réel.

Les violations de données humanitaires nuisent à l'action des organisations humanitaires et peuvent entraîner des risques considérables pour la dignité et la sécurité des personnes touchées par des conflits armés, des catastrophes et d'autres situations d'urgence.

Alors que le Mouvement met en œuvre des mesures pour protéger les personnes dont les données ont été corrompues et travaille à reconstruire l'infrastructure informatique compromise, cette résolution du Conseil des Délégués vise à renforcer le cadre politique et juridique de protection des données et de l'infrastructure numérique d'organisations humanitaires impartiales. Elle offre une base aux travaux collectifs du Mouvement vers un consensus ferme – en mots comme en actes – quant au fait que les données humanitaires ne doivent jamais être corrompues, et que les activités humanitaires doivent être protégées en ligne, de la même manière qu'elles le sont hors ligne.

1) INTRODUCTION

Au début de l'année 2022, le CICR a découvert que des serveurs hébergeant les données personnelles de plus de 500 000 bénéficiaires de services du Mouvement étaient compromis, du fait d'une violation de données élaborée[2]. Bien que cela ait été un choc, il ne s'agit pas d'un phénomène rare, mais au contraire du reflet d'une tendance croissante dans les cyberopérations visant des organisations humanitaires.

Les cyberopérations à l'encontre d'organisations humanitaires peuvent avoir de graves conséquences pour les personnes vulnérables. La violation des données à l'encontre du Mouvement, par exemple, a concerné les 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 consultées pourraient être utilisées par certains États, groupes non étatiques ou 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 les données humanitaires risquent de perturber les opérations d'organisations humanitaires et d'éroder la confiance dans leur action. La confiance est indispensable au fonctionnement des organisations humanitaires, et une violation des données risque de mettre en péril leur accès aux personnes ayant besoin d'aide, ainsi que la sécurité de leurs équipes et de leurs opérations, et au final d'aggraver encore la situation des personnes touchées par des conflits armés, des catastrophes naturelles ou d'autres situations d'urgence.

Alors que le Mouvement élabore des mesures visant à protéger les personnes dont les données ont

[1] Pour en savoir plus, consultez l'adresse https://www.icrc.org/fr/document/cyberattaque-cicr-ce-que-nous-savons.
[2] *Ibid*.

été corrompues et œuvre pour reconstruire l'infrastructure informatique compromise, cette résolution vise à renforcer le cadre politique et juridique de protection des données et de l'infrastructure numérique d'organisations humanitaires impartiales. Elle offre un fondement aux travaux collectifs du Mouvement vers un consensus ferme – en mots comme en actes – quant au fait que les données humanitaires ne doivent jamais être corrompues, et que les activités humanitaires doivent être protégées en ligne, de la même manière qu'elles le sont hors ligne.

La résolution représente aussi l'étape suivante dans les travaux juridiques, politiques et techniques du Mouvement relatifs à la protection des données et des opérations humanitaires, s'appuie sur la résolution 4 de la XXXIII[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale) et sert de tremplin vers l'adoption possible d'une autre résolution pendant la XXXIV[e] Conférence internationale.

2) CONTEXTE

La résolution est le résultat des efforts conjoints du CICR, de la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Fédération internationale) et de plusieurs Sociétés nationales en vue de faire face à la violation des données qui a eu lieu en 2022. Elle envoie un message fort aux États, aux autres acteurs et à d'autres organisations humanitaires impartiales concernant l'importance de la protection des données humanitaires.

Cette résolution étant présentée en réaction à la violation des données survenue en 2022, toutes les composantes du Mouvement ont été invitées et encouragées à prendre part à un ensemble de consultations accélérées organisées en mars et avril 2022, conformément au calendrier suivant :

- mi-mars 2022 : diffusion de l'avant-projet de résolution auprès de toutes les composantes du Mouvement ;
- fin mars 2022 : consultations informelles en ligne ouvertes à toutes les composantes du Mouvement ;
- 8 avril 2022 : délai pour la soumission par les composantes du Mouvement de commentaires écrits concernant l'avant-projet de résolution ;
- début mai 2022 : envoi officiel par courrier électronique de tous les documents du Conseil des Délégués, y compris un projet final de résolution sur la protection des données humanitaires.

Afin de débattre du projet de résolution, les composantes du Mouvement sont encouragées à contacter :

- Tilman Rodenhäuser, conseiller juridique, CICR, trodenhauser@icrc.org, ou ;
- Mathilde Piret, conseillère juridique, CICR, mpiret@icrc.org.

3) ANALYSE

La violation des données survenue en 2022 a mis en lumière les risques que les cyberopérations, et notamment les violations de données, peuvent entraîner pour les organisations humanitaires, y compris pour le Mouvement. Depuis plusieurs années, le CICR et d'autres composantes du Mouvement avertissent de la nécessité vitale et urgente pour les États et d'autres acteurs de protéger les données humanitaires et l'infrastructure numérique des cyberopérations, intrusions et usages abusifs de données. La récente violation dont ont fait l'objet des données personnelles a malheureusement montré que ce risque n'est que trop réel.

La consultation ou l'extraction non autorisée de données ayant été recueillies, conservées ou traitées d'une autre manière par des organisations humanitaires impartiales nuit à leur action et peut entraîner des risques considérables pour la dignité et la sécurité des personnes touchées par des

conflits armés, des catastrophes ou d'autres situations d'urgence. Tandis que les technologies numériques reposent sur des systèmes informatiques pour leur fonctionnement, la priorité du Mouvement devrait toujours être centrée sur les personnes, en particulier les plus vulnérables.

Aux fins de la résolution, nous suggérons de définir les « données humanitaires » comme les données, y compris personnelles, traitées (par exemple recueillies, conservées, transférées ou archivées) à des fins humanitaires par des organisations humanitaires impartiales. Ces données peuvent inclure les données personnelles de personnes ayant besoin de services humanitaires, mais aussi des données non personnelles recueillies dans le contexte d'opérations humanitaires, comme des rapports de visites de lieux de détention, des rapports sur les besoins des populations touchées par des conflits armés, des catastrophes ou d'autres situations d'urgence, et les données nécessaires à la planification de l'assistance humanitaire.

Le renforcement de la cybersécurité, de la sécurité des données et de la protection des données personnelles au sein du Mouvement et dans le secteur humanitaire au sens large est un objectif de long terme, qui requiert l'adoption de mesures juridiques, politiques et techniques. Afin d'atteindre cet objectif, les composantes du Mouvement ont accès à plusieurs outils, comme le programme de formation et de certification destiné aux responsables de la protection des données dans l'action humanitaire, dirigé par le Bureau de la protection des données du CICR et l'Université de Maastricht. Le projet de résolution relatif à « La protection des données humanitaires » est un autre élément de la réaction du Mouvement à cet égard. Ce dernier poursuivra des objectifs divers et interconnectés, et notamment :

- attirer l'attention sur les risques croissants des cyberopérations à l'encontre d'organisations humanitaires et sur les conséquences négatives des violations de données, et insister sur la valeur des données humanitaires et sur la nécessité de les protéger ;
- faire passer le message selon lequel les violations visant les données confiées à des organisations humanitaires :
    - nuisent à la préservation de la vie privée, à la dignité et à la sécurité des personnes vulnérables et les expose à des risques considérables, y compris à des atteintes physiques et psychologiques ;
    - portent préjudice à la confiance placée dans ces organisations, et à l'action humanitaire impartiale en général, et risquent de perturber leurs opérations et de menacer les efforts qu'elles déploient pour soulager les souffrances humaines ;
- réaffirmer l'engagement du Mouvement à mettre en œuvre des règles en matière de protection des données et des mesures de cybersécurité, à garantir des pratiques efficaces à cet égard et à les respecter ;
- faciliter les activités, dans l'ensemble du Mouvement, ayant pour objectif le partage de bonnes pratiques, le renforcement des capacités de toutes les composantes du Mouvement, et la réflexion concernant l'élaboration conjointe d'un Code de conduite du Mouvement relatif à la protection des données, ainsi que la création d'un groupe de travail informel à cette fin ;
- impliquer le Mouvement sur cette question et envoyer un message fort d'engagement du Mouvement aux États, à d'autres acteurs et à d'autres organisations humanitaires impartiales au sujet de :
    - la responsabilité des organisations humanitaires s'agissant de prendre des mesures concrètes et efficaces pour garantir la sécurité des données et protéger les données personnelles qui leur sont confiées ;
    - la responsabilité des États de respecter et de protéger les organisations humanitaires et leur personnel, informations et avoirs, tant en ligne que hors ligne ;
    - la nécessité pour les composantes du Mouvement de travailler avec d'autres organisations humanitaires et avec des partenaires pour renforcer la cybersécurité et pour mettre en place ou acquérir les solutions appropriées qui renforcent les mécanismes de prévention contre de telles attaques, et qui limitent leurs conséquences, le cas échéant ;

- harmoniser l'action du Mouvement autour d'un intérêt commun en vue de rechercher et concevoir des mesures pour préserver un espace humanitaire neutre, indépendant et impartial dans la sphère numérique, comme les recherches menées par le CICR sur un emblème numérique[3].

4) INCIDENCES FINANCIÈRES

En adoptant la présente résolution, les composantes du Mouvement s'engagent à prendre des mesures appropriées, dans les limites de leurs capacités et de leurs besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau de sécurité suffisamment élevé lorsqu'elles traitent des données (par exemple les recueillir, les conserver ou les transférer) afin de mener leurs activités, se conformer à la législation et aux cadres applicables en matière de protection des données personnelles, et pour observer les normes et les meilleures pratiques pertinentes lors du traitement de données personnelles, tout en tenant compte du *Manuel sur la protection des données dans l'action humanitaire*.

Les composantes du Mouvement seront aussi invitées à rejoindre un groupe de travail informel pour partager les bonnes pratiques en matière de sécurité des données et de protection des données personnelles, s'apporter un soutien mutuel dans le renforcement des capacités, s'assurer que les employés et les volontaires ont conscience de l'importance de la sécurité et de la protection des données, et de la façon dont chacun peut et devrait contribuer à cet objectif, ainsi que pour réfléchir à la possibilité d'élaborer un Code de conduite du Mouvement relatif à la protection des données.

En outre, la résolution proposée encourage le CICR et d'autres composantes du Mouvement à mener des recherches et à concevoir des mesures pour préserver un espace humanitaire neutre, indépendant et impartial dans la sphère numérique. Elle encourage également le CICR à consulter les composantes du Mouvement et à coordonner ses activités et les leurs dans la poursuite de ses recherches sur la faisabilité technique d'un emblème numérique et à évaluer ses bénéfices.

La mise en œuvre de ces engagements est susceptible d'avoir des incidences sur le plan financier pour les composantes individuelles du Mouvement, en fonction de l'ampleur de leurs programmes et activités existants, et du nombre d'employés déjà consacrés à cette question.

5) MISE EN ŒUVRE ET SUIVI

La réussite de cette résolution dépend de son application effective et cohérente par les composantes du Mouvement. Toutes les composantes du Mouvement sont censées mettre en œuvre et appliquer la résolution dans le cadre de leurs travaux en matière de sécurité des données et de protection des données personnelles, selon leurs moyens et en fonction des besoins.

Toutes les composantes du Mouvement sont invitées à soumettre des rapports au Conseil des Délégués de 2023 sur les progrès réalisés dans la mise en œuvre de cette résolution.

[3] Le concept d'emblème numérique est utilisé ici et dans le projet de résolution pour signifier « un emblème, un signe ou d'autres moyens numériques permettant d'identifier les données et infrastructures numériques des organisations et entités autorisées à utiliser les emblèmes distinctifs reconnus par le droit international humanitaire et de signaler, le cas échéant, la protection juridique qui leur est conférée ». L'idée est de créer un emblème, un signe ou d'autres moyens numériques d'identification qui joueront le rôle de protection et de signalement des emblèmes distinctifs tels qu'ils sont décrits au titre du droit international humanitaire.

Conclusion et recommandations

Au vu de la violation dont ont fait l'objet, en 2022, des données humanitaires détenues par le CICR et par plus de 60 Sociétés nationales, la résolution du Conseil des Délégués sur la protection des données humanitaires est un élément important de la réponse du Mouvement face à cette nouvelle menace qui évolue rapidement.

La résolution met en lumière les risques que les cyberopérations visant des données humanitaires entraînent pour les personnes dont les données personnelles sont corrompues, ainsi que pour les organisations humanitaires et leur capacité à remplir leurs missions d'aide et de protection des personnes touchées par des conflits armés, des catastrophes naturelles et d'autres situations d'urgence. Elle affirme également l'engagement du Mouvement à faire un usage responsable des nouvelles technologies et à s'efforcer de mettre en œuvre des règles en matière de protection des données et des mesures de cybersécurité, et elle envoie un message clair et fort aux États afin qu'ils respectent et protègent les organisations humanitaires, leur personnel, leurs données et leurs avoirs, tant en ligne que hors ligne.