

Le pouvoir de l'humanité

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

22-23 juin 2022, Genève



FR

CD/22/

Original : anglais

Projet

CONSEIL DES DÉLÉGUÉS

DU MOUVEMENT INTERNATIONAL DE LA CROIX-ROUGE ET DU CROISSANT-ROUGE

Genève, 22-23 juin 2022

La protection des données humanitaires

Avant-projet de résolution

**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**

Genève, mars 2022

AVANT-PROJET DE RÉSOLUTION

La protection des données humanitaires

Le Conseil des Délégués,

choqué et vivement préoccupé par la récente violation dont ont fait l'objet des données personnelles qui avaient été confiées au Comité international de la Croix-Rouge (CICR) et à diverses Sociétés nationales de la Croix-Rouge et du Croissant-Rouge,

notant avec inquiétude que la consultation ou l'extraction non autorisée de données traitées (par exemple collectées, conservées ou transférées) 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,

soulignant que de tels actes sont inacceptables, incompatibles avec la lettre et l'esprit du droit international humanitaire et contraires au consensus international établi de longue date quant à l'importance d'une action humanitaire impartiale,

réaffirmant que la capacité des organisations humanitaires impartiales à traiter des données personnelles ainsi que des données sensibles à caractère non personnel (données humanitaires) est une condition essentielle sur laquelle repose leur capacité à mettre en œuvre des activités humanitaires, telles que la fourniture de soins médicaux et de secours humanitaires, la protection des détenus et des civils, notamment de groupes particulièrement vulnérables comme les migrants et les enfants, la recherche de personnes disparues et la réunification de familles dispersées,

conscient qu'il est de la plus haute importance que les personnes puissent transmettre leurs données personnelles aux organisations humanitaires en toute confiance et que ces données soient protégées, et *rappelant* que la protection des données personnelles est étroitement liée à la préservation de la vie privée, de la dignité et de la sécurité des personnes,

soulignant la confiance que les États et les autres acteurs intervenant dans des conflits armés, des catastrophes naturelles ou d'autres situations d'urgence placent dans l'impartialité des organisations humanitaires et de leur action, ainsi que le fait que cette confiance est une condition préalable indispensable à l'accomplissement par ces organisations de leurs mandats et de leurs activités,

rappelant l'attachement du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) à ses Principes fondamentaux, et *reconnaissant* que ses composantes traitent des données dans le cadre des mandats et des rôles qui leur ont été conférés au titre du droit international humanitaire, des Statuts du Mouvement et des résolutions adoptées par la Conférence internationale de la Croix-Rouge et du Croissant-Rouge, en tenant dûment compte des cadres et principes en matière de protection des données, tels que ceux énoncés dans le *Manuel sur la protection des données dans l'action humanitaire* et le *Code de conduite relatif à la protection des données à caractère personnel pour les activités de rétablissement des liens familiaux*, ainsi que des cadres relatifs à la protection, tels que les *Standards professionnels pour les activités de protection*,

rappelant également la résolution 4 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 de la Croix-Rouge et du Croissant-Rouge,

1. *souligne* que la transformation numérique des activités menées par les organisations humanitaires, notamment le traitement des données humanitaires, va de pair avec la responsabilité pour ces organisations d'adopter des mesures de cybersécurité et des pratiques de protection des données afin d'atténuer les risques de violation des données – de manière à protéger les personnes dont les données sont traitées, l'organisation, son personnel et ses volontaires contre tout préjudice pouvant résulter de telles violations – ainsi que de prévoir des mesures d'urgence et des contre-mesures et de les appliquer si une violation de données devait néanmoins avoir lieu ;
2. *reconnaît* que, chaque fois qu'une organisation humanitaire traite des données humanitaires, elle devrait le faire uniquement à des fins compatibles avec son mandat purement humanitaire et dans le respect de la législation en vigueur ainsi que des cadres et principes applicables en matière de protection des données ;
3. *reconnaît également* combien il est essentiel que les États et les autres acteurs respectent la finalité humanitaire du traitement de ces données ;
4. *reconnaît en outre* que l'utilisation abusive de données personnelles traitées par des organisations humanitaires peut donner lieu à des violations des obligations relatives au respect de la vie privée inscrites dans les cadres juridiques nationaux, régionaux et internationaux, ainsi qu'à de graves violations des droits fondamentaux des personnes concernées ;
5. *note avec préoccupation* que les cyberopérations hostiles, notamment les violations de données, peuvent éroder la confiance placée dans les organisations humanitaires impartiales et que, cette confiance leur étant indispensable pour pouvoir agir, ces violations risquent 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 ;
6. *exprime son inquiétude* face aux cyberopérations qui perturbent l'action des organisations humanitaires impartiales ainsi qu'à la désinformation qui sape la confiance dans leurs activités et met leur personnel en danger ;
7. *réaffirme* l'importance essentielle de l'obligation qu'ont, au titre du droit international humanitaire, toutes les parties à un conflit armé d'autoriser et de faciliter dans ces situations la conduite d'activités humanitaires impartiales ainsi que de respecter et de protéger l'action et le personnel humanitaires ;
8. *souligne* 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 ;
9. *encourage* le CICR, les composantes du Mouvement et autres organisations humanitaires, les États et les experts en la matière à rechercher et concevoir des mesures pour préserver un espace humanitaire neutre, indépendant et impartial dans la sphère numérique ;
10. *encourage* le CICR à poursuivre ses recherches sur la faisabilité technique d'un emblème numérique – autrement dit, un emblème ou un signe distinctif 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 – et à évaluer les avantages d'un tel signe ou emblème, ainsi qu'à assurer la coordination avec la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Fédération internationale) et les Sociétés nationales et à mener des consultations avec les États et des experts dans cette optique ;

11. *engage* les composantes du Mouvement et *appelle* les autres organisations humanitaires 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, pour appliquer les meilleures pratiques de gouvernance des données à l'ensemble des données humanitaires, pour se conformer à la législation en vigueur 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* ;
12. *invite* le CICR et la Fédération internationale à faire rapport au Conseil des Délégués de 2023 sur les mesures adoptées par les composantes du Mouvement pour assurer la sécurité des données et la protection des données personnelles ;
13. *appelle* les États et les autres acteurs à respecter et protéger les organisations humanitaires impartiales en ligne comme elles le font hors ligne, notamment en les préservant de toute opération d'information ou cyberopération hostiles, et *demande* aux États de faire en sorte que les acteurs sur lesquels ils ont une influence respectent les organisations humanitaires et leurs données, et de prendre toutes les mesures possibles pour protéger les personnes dont les données ont fait l'objet d'une violation ;
14. *appelle également* les États et les autres acteurs – en particulier les communautés d'experts, les chercheurs et le secteur privé – à collaborer avec les organisations humanitaires et à les soutenir afin qu'elles puissent développer ou se procurer les outils et les infrastructures nécessaires pour assurer la sécurité et la protection de leurs données humanitaires ;
15. *envisage* d'examiner la question de la sécurité et de la protection des données humanitaires dans le cadre de la XXXIV^e Conférence internationale de la Croix-Rouge et du Croissant-Rouge.