



Le pouvoir de l'humanité

XXXIV^e Conférence internationale
de la Croix-Rouge et du Croissant-Rouge

28-31 octobre 2024, Genève

Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés

PROJET DE RÉOLUTION

Septembre 2024

FR

34IC/24/9.2DR
Original : anglais
Pour décision

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

PROJET DE RÉSOLUTION

Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés

La XXXIV^e Conférence internationale de la Croix-Rouge et du Croissant-Rouge,

reconnaissant que nous vivons dans un monde de plus en plus numérisé et connecté, ce qui ouvre des perspectives dans les domaines social, économique, humanitaire, du développement ainsi que de l'information et de la communication, et peut contribuer à sauver des vies et à améliorer les conditions d'existence, y compris dans les situations de conflit armé,

soulignant l'importance de la connectivité et des technologies de l'information et de la communication (ou technologies numériques) pour assurer la fourniture de biens et services essentiels – en particulier la nourriture, l'eau, l'électricité, le chauffage, l'assainissement ainsi que les services médicaux et humanitaires – à la population civile et aux autres personnes protégées, et pour permettre aux civils, d'une part, de rechercher et recevoir des informations dans un format accessible sur les lieux où ils peuvent se mettre en sécurité et trouver des biens indispensables à leur survie et, d'autre part, de rester en contact avec leurs proches, y compris dans les situations de conflit armé,

rappelant qu'il est de plus en plus probable que les technologies numériques soient utilisées dans des conflits futurs entre États, et *notant* que ces technologies, en particulier celles facilitant la conduite d'opérations d'information, ont déjà été utilisées dans des conflits armés survenus dans différentes régions du monde,

notant avec inquiétude que l'utilisation de capacités numériques par les parties aux conflits armés peut causer des dommages aux civils ainsi qu'aux autres personnes et biens protégés, y compris par-delà les frontières internationales, en particulier lorsqu'elle vise, ou affecte incidemment, des systèmes informatiques intégrés à des biens de caractère civil, notamment des infrastructures civiles critiques ou fournissant des services essentiels, ou des ouvrages et installations contenant des forces dangereuses,

notant également avec inquiétude qu'un manque de capacités adéquates pour détecter les activités numériques malveillantes et s'en défendre peut rendre les États et les composantes du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) plus vulnérables,

se déclarant préoccupée par l'ampleur, la vitesse de propagation et la portée de la désinformation, des discours de haine et autres informations nocives véhiculés au moyen des technologies numériques, en particulier des plateformes de médias sociaux, ainsi que par les dommages qu'une telle utilisation de ces technologies risque d'infliger en période de conflit armé à la population civile et aux autres personnes protégées, notamment lorsqu'elles sont employées pour enrôler des enfants dans des forces armées,

reconnaissant que les activités numériques peuvent affecter chaque personne différemment, selon qu'il s'agisse d'une femme, d'un homme, d'une fille ou d'un garçon, et en fonction aussi de son âge, de son handicap éventuel et de son milieu social,

notant avec préoccupation que l'utilisation de l'intelligence artificielle et d'autres technologies émergentes dans le cadre d'activités numériques malveillantes peut accroître leur portée et leur vitesse, ainsi que les dommages qu'elles sont susceptibles de causer,

notant que les technologies numériques permettent à des civils de mener ou soutenir des activités numériques dans des situations de conflit armé, ou sont utilisées pour les encourager à mener ou soutenir de telles activités dans ces situations, et *s'inquiétant* de ce que les civils ne soient pas toujours au fait des risques encourus ni des limites juridiques applicables à leur conduite,

rappelant que les entreprises technologiques privées fournissent tout un éventail de produits, de services et d'infrastructures numériques dont dépendent les civils, les gouvernements et les organisations humanitaires, y compris en période de conflit armé, et *soulignant* l'importance que revêt la disponibilité de ces produits, services et infrastructures pour la population civile,

reconnaissant que les technologies numériques sont essentielles pour la conduite d'opérations humanitaires efficaces et efficientes, et *exprimant de vives inquiétudes* quant aux conséquences qu'ont les activités numériques pour les organisations humanitaires, notamment les violations de données et les opérations de désinformation dont elles sont la cible, perturbant leurs opérations de secours, sapant la confiance dans les organisations humanitaires, y compris les composantes du Mouvement, et menaçant la sûreté et la sécurité de leur personnel, de leurs locaux et de leurs biens ainsi que, en fin de compte, leur accès et leur capacité à mener des activités humanitaires,

rappelant la valeur juridique et protectrice des signes et signaux distinctifs, et *prenant note avec intérêt* des recherches en cours sur la finalité, les paramètres et la faisabilité d'un emblème numérique, menées par le Comité international de la Croix-Rouge (CICR) en collaboration avec des établissements universitaires et d'autres composantes du Mouvement,

réaffirmant la résolution 4 adoptée par la XXXIII^e Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale) et intitulée « Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles », et *soulignant* que les questions abordées dans cette résolution sont importantes également du point de vue de la protection des autres données humanitaires,

prenant note de la résolution 12 adoptée par le Conseil des Délégués de 2022 et intitulée « La protection des données humanitaires », *saluant* les engagements pris par le Mouvement en ce qui concerne la protection de ses données humanitaires, notamment en vue de renforcer ses capacités en la matière, et *insistant* sur l'importance d'assurer la confidentialité, l'intégrité et la disponibilité des données pour les opérations humanitaires,

prenant note également de la résolution 76/19 de l'Assemblée générale des Nations Unies et du travail accompli par les États dans le cadre du Groupe de travail des Nations Unies à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025),

appelant les États à s'abstenir, dans le cadre de l'utilisation qu'ils font des technologies numériques, de prendre des mesures dérogeant au droit international, en particulier à la Charte des Nations Unies, qui prévoit notamment l'obligation de régler les différends internationaux par des moyens pacifiques et l'interdiction de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies, *réaffirmant* sa conviction

qu'aucune disposition du droit international humanitaire (DIH) ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force, et *soulignant* que le rappel du DIH ne légitime ni n'encourage en aucun cas les conflits armés,

reconnaissant que les caractéristiques propres à l'environnement numérique soulèvent des questions quant à la manière dont certains principes et certaines règles du DIH s'appliquent dans les situations de conflit armé, et que les avis des États divergent sur ces questions,

soulignant le fait que les personnes et les infrastructures critiques, ainsi que les organisations médicales et humanitaires, sont exposées en tout temps au risque de subir des dommages causés par des activités numériques, *appelant* les États à prendre appui sur cette résolution pour mettre en place des mesures efficaces visant à assurer leur protection conformément aux cadres juridiques applicables et en fonction des capacités numériques dont ils disposent, et *demandant* au Mouvement de prendre des mesures appropriées pour assurer en tout temps la sécurité numérique et la protection des données,

1. *exprime* la volonté commune à tous les membres de la Conférence internationale de protéger les civils ainsi que les autres personnes et biens protégés dans les situations de conflit armé, y compris contre les dangers résultant des activités numériques ;
2. *rappelle* que le DIH s'applique uniquement aux situations de conflit armé – de même que les principes reconnus du droit international que sont l'humanité, la nécessité, la proportionnalité et la distinction – et que, dans ces situations, le DIH ne s'applique qu'aux actes qui sont commis dans le cadre du conflit et qui sont liés à celui-ci ;
3. *reconnaît* la nécessité d'examiner plus avant de quelle manière et dans quelles circonstances ces principes s'appliquent à l'utilisation des technologies numériques, *souligne* que le rappel de ces principes ne légitime ni n'encourage en aucun cas les conflits armés, *demande instamment* aux États de s'accorder à ce sujet, tout en notant par ailleurs la possibilité d'établir à l'avenir de nouvelles obligations contraignantes, le cas échéant ;
4. *réitère* que, dans les situations de conflit armé, les règles et principes du DIH – notamment le principe de distinction, l'interdiction de lancer des attaques indiscriminées ou disproportionnées, l'obligation de veiller constamment, lors de la conduite des opérations militaires, à épargner la population civile, les personnes civiles et les biens de caractère civil et à prendre toutes les précautions pratiquement possibles en vue d'éviter et, en tout cas, de réduire au minimum les dommages causés incidemment aux civils, l'interdiction d'encourager ou d'inciter à commettre des violations du DIH, et l'interdiction de se livrer à des actes ou menaces de violence dont le but principal est de répandre la terreur parmi la population civile – contribuent à protéger les civils ainsi que les autres personnes et biens protégés, notamment contre les dangers liés aux activités numériques ;
5. *appelle* les parties aux conflits armés à protéger, conformément aux obligations qui leur incombent au titre du droit international, les infrastructures critiques qui fournissent des services dans plusieurs États, comme les infrastructures techniques essentielles à la disponibilité générale ou à l'intégrité d'Internet, en particulier les câbles sous-marins et les réseaux de communication satellitaire ;
6. *appelle également* les parties aux conflits armés à respecter et protéger, conformément aux obligations qui leur incombent au titre du droit international, le personnel médical ainsi que les unités et moyens de transport sanitaires, y compris dans le cadre de leurs activités numériques ;

7. *appelle* les États et les parties aux conflits armés à autoriser et faciliter, dans les situations de conflit armé, la conduite d'activités humanitaires impartiales, notamment celles reposant sur des technologies numériques, et à respecter et protéger, conformément aux obligations qui leur incombent au titre du droit international, le personnel et les biens humanitaires, y compris dans le cadre de leurs activités numériques ;
8. *demande instamment* aux États et aux parties aux conflits armés de protéger efficacement, conformément aux obligations qui leur incombent au titre du droit international, les civils ainsi que les autres personnes et biens protégés, y compris dans le cadre de leurs activités numériques ;
9. *appelle* les États, ainsi que les composantes du Mouvement s'il y a lieu et en fonction de leurs mandats respectifs, à diffuser le DIH le plus largement possible sur leur territoire, de telle manière que les principes en soient connus de l'ensemble de la population, *invite instamment* les États à prendre des mesures pour prévenir les violations du DIH, et *rappelle* que les États se sont engagés à prendre les mesures nécessaires pour faire cesser les violations du DIH, notamment à mener des enquêtes et à engager des poursuites lorsqu'il y a lieu ;
10. *encourage* toutes les composantes du Mouvement à tenir compte des dommages que les activités numériques peuvent causer aux civils ainsi qu'aux autres personnes et biens protégés, leur *demande instamment* de renforcer leur préparation et leur capacité à faire face aux risques liés à ces activités – sachant que ces dernières peuvent affecter différents groupes de personnes de différentes manières –, par exemple en améliorant leur capacité à détecter ces risques et à prévenir les dommages causés aux civils, et *invite* les États à soutenir le Mouvement dans ces efforts ;
11. *encourage* les États, ainsi que les composantes du Mouvement s'il y a lieu et en fonction de leurs mandats respectifs, à adopter des mesures pour faire prendre conscience aux entreprises technologiques privées relevant de leur champ de compétence que le fait de fournir des services numériques à des clients qui participent ou peuvent être appelés à participer à un conflit armé implique certains risques, et à établir, s'il y a lieu, un dialogue avec ces entreprises pour les encourager à en apprendre davantage sur ces risques ainsi qu'à adopter, si nécessaire, des mesures pour informer leur personnel, le protéger face à ces risques et lui permettre d'agir en conformité avec le droit applicable ;
12. *encourage* le CICR à continuer de mener des consultations et de dialoguer activement avec les États et les composantes du Mouvement pour évaluer et établir plus précisément la finalité spécifique et la faisabilité technique d'un emblème numérique, à fournir, dans la mesure du possible, aux composantes du Mouvement et aux États intéressés un soutien quant à l'utilisation qui pourrait être faite d'un tel emblème dans le cadre d'un conflit armé, et à examiner les démarches juridiques et diplomatiques pouvant être entreprises dans cette optique ;
13. *engage* les composantes du Mouvement à prendre des mesures appropriées, dans les limites de leurs mandats, possibilités et besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de sécurité numérique et de protection des données, conformément à la résolution 12 adoptée par le Conseil des Délégués de 2022 et intitulée « La protection des données humanitaires », et *invite* les États à soutenir le Mouvement dans ces efforts ;
14. *rappelle* que les composantes du Mouvement doivent traiter des données personnelles pour pouvoir s'acquitter de leurs mandats, notamment au titre du DIH, lorsqu'il s'applique, et des Statuts du Mouvement, et que ce traitement est nécessaire et justifié

par des motifs importants d'intérêt public ainsi que par les intérêts vitaux des personnes concernées, et *engage instamment* les États et le Mouvement à coopérer pour veiller à ce que ces données ne soient pas sollicitées ni utilisées à des fins incompatibles avec la nature humanitaire de l'action du Mouvement ou d'une manière susceptible de nuire à la confiance des personnes auxquelles il vient en aide ou à l'indépendance, l'impartialité et la neutralité de ses opérations ;

15. *encourage* les États et les composantes du Mouvement à échanger leurs connaissances et leurs bonnes pratiques et à renforcer leurs capacités en matière de sécurité numérique, de protection des données, de droit international et de protection des civils, ainsi que des autres personnes et biens protégés, contre les dangers liés aux activités numériques, en tenant compte des disparités qui existent au niveau des ressources dont disposent les États et les composantes du Mouvement.