



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

RÉSOLUTION

Octobre 2024

FR

34IC/24/R2
Original : anglais
Adoptée

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 fournir divers biens et services, en particulier les services médicaux destinés à la population civile, pour mener les opérations humanitaires, pour permettre aux civils 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 pour maintenir ou rétablir les liens familiaux, 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, et *notant* que ces technologies ont déjà été utilisées dans des conflits armés survenus dans différentes régions du monde,

rappelant également la ratification universelle des Conventions de Genève de 1949, et *soulignant* la responsabilité première qui incombe aux États en matière de développement du droit international humanitaire (DIH),

reconnaissant la résolution 76/19 de l'Assemblée générale des Nations Unies et le travail accompli par les États dans le cadre du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), ainsi que le fait que la Première Commission de l'Assemblée générale des Nations Unies, plus particulièrement le Groupe de travail à composition non limitée (2021-2025), est un forum intergouvernemental essentiel pour étudier la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États,

rappelant que la Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale) a pour attribution de contribuer au respect et au développement du DIH,

notant avec inquiétude que l'utilisation malveillante 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 biens indispensables à la survie de la population civile, des ouvrages et installations contenant des forces dangereuses, ou des infrastructures civiles critiques,

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,

notant l'ampleur, la vitesse et la portée de la propagation des activités numériques malveillantes, en particulier par le biais des plateformes de médias sociaux, et *se déclarant préoccupée* par le fait que ce phénomène puisse infliger des dommages à la population civile et aux autres personnes et biens protégés en période de conflit armé, favoriser de tels dommages ou les aggraver, notamment lorsque les technologies numériques sont utilisées pour enrôler des enfants dans les forces armées,

reconnaissant que les conflits armés peuvent affecter différemment les femmes, les hommes, les filles et les garçons, en fonction aussi de leur âge, de leur handicap éventuel et de leur milieu social, et que ces différences doivent être prises en compte dans la mise en œuvre et l'application du DIH, afin d'assurer à tous une protection adéquate,

reconnaissant également que l'intelligence artificielle et d'autres technologies émergentes peuvent apporter à la population civile des bienfaits sur le plan humanitaire, social, économique et du développement, mais *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 peuvent permettre à des civils de mener ou soutenir des activités numériques dans des situations de conflit armé, ou être 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 et conséquences 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, *soulignant* l'importance que revêt la disponibilité et l'intégrité de ces produits, services et infrastructures pour la population civile, et *relevant* qu'il est également important que les entreprises technologiques privées prennent en compte les besoins de toutes les personnes touchées par un conflit armé, dans le respect du droit applicable,

reconnaissant que les technologies numériques sont essentielles pour la conduite d'opérations humanitaires efficaces et efficientes, et *exprimant de vives inquiétudes* quant aux conséquences que peuvent avoir les activités numériques malveillantes 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* 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 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,

rappelant que les États ne doivent prendre aucune mesure 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 DIH ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies, 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 les principes et les règles du DIH s'appliquent aux activités numériques dans les situations de conflit armé, et que les avis des États divergent sur ces questions, ce qui témoigne de la nécessité de poursuivre les discussions à cet égard,

soulignant le fait que les personnes et les infrastructures critiques, ainsi que les organisations médicales et humanitaires et leur personnel, sont exposés en tout temps au risque de subir des dommages causés par des activités numériques, et *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,

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 risques résultant des activités numériques malveillantes ;
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 uniquement 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, et *demande instamment* aux États de s'accorder à ce sujet ;
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, lors de la conduite des opérations militaires, d'épargner la population civile, les personnes civiles et les biens de caractère civil et de 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 risques résultant des activités numériques ;

5. *appelle* les parties aux conflits armés à protéger, conformément aux obligations qui leur incombent au titre du droit international, les infrastructures civiles critiques qui fournissent des services dans plusieurs États, y compris 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, conformément aux obligations qui leur incombent au titre du droit international, les civils ainsi que les autres personnes et biens protégés – notamment les monuments historiques, les œuvres d'art et les lieux de culte qui constituent le patrimoine culturel ou spirituel des peuples –, 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, et *invite instamment* les États à prendre des mesures pour prévenir et réprimer les violations du DIH, notamment à mener des enquêtes et à engager des poursuites lorsqu'il y a lieu, conformément aux obligations qui leur incombent au titre du droit international, y compris dans le cadre de leurs activités numériques ;
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 également* toutes les composantes du Mouvement, s'il y a lieu et en fonction de leurs mandats respectifs, à diffuser le DIH auprès des entreprises technologiques privées et à leur faire prendre conscience 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, ainsi qu'à établir, s'il y a lieu, un dialogue avec ces entreprises pour les encourager à envisager d'adopter des mesures afin de prendre en compte les besoins de toutes les personnes touchées par un conflit armé, dans le respect du droit interne et du droit international applicables ;
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 ; 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 étudier les démarches juridiques et diplomatiques pouvant être entreprises dans cette optique ;

13. *encourage* les États et les composantes du Mouvement à échanger leurs connaissances et leurs bonnes pratiques, à établir des contacts et des réseaux de communication pour promouvoir la coopération internationale et à les renforcer, et à développer 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 risques résultant des activités numériques malveillantes, en tenant compte des disparités qui existent au niveau des ressources dont disposent les États et les composantes du Mouvement.