RFC 8280 : Research into Human Rights Protocol Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 novembre 2017

Date de publication du RFC : Octobre 2017

https://www.bortzmeyer.org/8280.html

Ce RFC très politique est le premier du groupe de recherche IRTF <https://irtf.org/hrpc> HRPC, dont le nom veut dire « Human Rights and Protocol Considerations ». À première vue, il n'y a pas de rapport entre les droits humains et les protocoles réseau. Les premiers relèvent de la politique, les seconds de la pure technique, non ? Mais, justement, le groupe HRPC a été créé sur la base de l'idée qu'il y a de la politique dans le travail de l'IETF, que les protocoles ne sont pas complètement neutres, et qu'il était nécessaire de creuser cette relation complexe entre protocoles et droits humains. Le premier RFC analyse le problème de base : « TCP/IP est-il politique ? »

Si vous êtes un concepteur de protocoles, plutôt porté sur le concret, et que les discussions politiques vous gonflent, vous pouvez passer directement à la section 6 du RFC, qui est la "*check-list*" Droits Humains pour votre prochain protocole ou format. En la suivant, vous pourrez plus facilement vérifier que votre création n'a pas trop d'effets néfastes, question droits humains. (Depuis, il vaut mieux consulter le RFC 9620 [1], qui la remplace.)

Ce RFC n'est pas le premier RFC « politique », et il ne faudrait pas croire que les ingénieur·e·s qui participent à l'IETF sont tou·[Caractère Unicode non montré [2]]e·s des "*nerds*" asociaux avec la conscience politique d'un poisson rouge. Parmi les RFC politiques, on peut citer le RFC 1984 (refus d'affaiblir la cryptographie), le RFC 7258 (post-Snowden, RFC affirmant que la surveillance de masse est une attaque contre l'Internet, et qu'il faut déployer des mesures techniques la rendant plus difficile), et bien sûr l'excellent RFC 6973, sur la vie privée, qui sert largement de modèle à notre RFC 8280.

Le groupe de recherche IRTF <https://irtf.org/hrpc> HRPC va donc travailler sur deux axes (section 3 de notre RFC) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9620.txt
2. Car trop difficile à faire afficher par LaTeX

— Est-ce que les protocoles Internet ont des conséquences en matière de droits humains et, si oui, comment ?
— Si la réponse à la première question est positive, est-il possible d'améliorer ces protocoles, afin de faire en sorte que les droits humains soient mieux protégés ?

Ce RFC particulier a eu une gestation de plus de deux ans <https://datatracker.ietf.org/doc/rfc8280/>. Deux des étapes importantes avaient été la réunion IETF 92 à Dallas <https://www.ietf.org/meeting/92/index.html>, et la réunion IETF 95 à Buenos Aires <https://www.ietf.org/meeting/95/index.html>. À la seconde, vu les opinions politiques de beaucoup des participant·e·s, l'après-réunion s'est tenu dans un restaurant végétarien. En Argentine...

La section 1 du RFC rappelle les nombreux débats qui ont agité le monde de l'Internet sur le rôle politique de ce réseau. Deux belles citations ouvrent cette section, une de Tim Berners-Lee qui dit « "*There's a freedom about the Internet : As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere.*" » et un extrait du RFC 3935 « "*The Internet isn't value-neutral, and neither is the IETF.*" ». Et le RFC 3935 continue : « "*We want the Internet to be useful for communities that share our commitment to openness and fairness. We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community. These concepts have little to do with the technology that's possible, and much to do with the technology that we choose to create.*" ». Le succès immense de l'Internet, contre tous les prophètes de malheur qui prétendaient que ce réseau, qui n'avait pas été conçu par des Messieurs Sérieux, ne pourrait jamais marcher, fait que l'impact social et politique des techniques de la famille TCP/IP est énorme. On trouve donc logiquement de nombreux textes qui affirment que « ce grand pouvoir donne à l'Internet de grandes responsabilités <https://en.wikiquote.org/wiki/Responsibility> », par exemple cette résolution des Nations Unies <https://documents-dds-ny.un.org/doc/UNDOC/LTD/N13/576/77/PDF/N1357677.pdf?OpenElement>, ou bien la déclaration de NETmundial <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>. Une position plus radicale est qu'il faut défendre et renforcer l'Internet, car il serait intrinsèquement un outil aux services des droits humains.

En effet, la connectivité de bout en bout, tout le monde peut parler à tous ceux qui veulent bien, Alice et Bob peuvent échanger sans autorisation, est à la fois un principe fondamental de l'Internet (cf. RFC 1958) et un puissant soutien aux droits humains. Pour citer Benjamin Bayart, « L[Caractère Unicode non montré]imprimerie a permis au peuple de lire, Internet va lui permettre d[Caractère Unicode non montré]écrire. » L'architecture de l'Internet est ouverte (je me souviens de techniciens d'un opérateur de télécommunications historique qui avaient poussé des cris d'horreur quand je leur avais montré traceroute, au début des années 1990. Ils avaient tout de suite demandé comment empêcher le client de regarder l'intérieur du réseau de l'opérateur.) Les normes techniques de l'Internet sont développées selon un processus ouvert, et sont librement distribuées (ce que ne font toujours pas les dinosaures de la normalisation comme l'AFNOR ou l'ISO). En prime, une bonne partie de l'infrastructure de l'Internet repose sur du logiciel libre.

L'Internet a prouvé qu'il pouvait continuer à fonctionner en environnement hostile (RFC 1984 et RFC 3365). Les RFC politiques cités plus haut défendent tous des valeurs qui vont dans le sens des droits humains (par exemple la vie privée, dans les RFC 6973 et RFC 7258). Cela ne va pas de soi : une organisation comme l'UIT n'en a jamais fait autant et développe au contraire des technologies hostiles aux droits humains comme les techniques de surveillance dans le NGN.

On pourrait peut-être même dire que non seulement l'Internet défend les droits humains, mais que ceux-ci sont à la base de l'architecture de l'Internet. (Cf. Cath, C. and L. Floridi, « "*The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights*" <https://link.springer.com/article/10.1007/s11948-016-9793-y> », 2017.) On peut citer ici Bless, R. et C. Orwat, « "*Values and Networks*" <https://dl.acm.org/citation.cfm?id=2935640> » : « "*to a*

certain extent, the Internet and its protocols have already facilitated the realization of human rights, e.g., the freedom of assembly and expression. In contrast, measures of censorship and pervasive surveillance violate fundamental human rights." » ou bien Denardis, L., « *"The Internet Design Tension between Surveillance and Security"* <http://ieeexplore.ieee.org/document/7116471/?reload=true&arnumber=7116471> » « *"Since the first hints of Internet commercialization and internationalization, the IETF has supported strong security in protocol design and has sometimes served as a force resisting protocol-enabled surveillance features.*" ».

Mais la question reste chaudement débattue à l'IETF. Nombreux sont les techniciens qui grommelent « tout ça, c'est de la politique, cela ne nous concerne pas », voire reprennent l'argument classique de la neutralité de la technique « un outil est neutre, c'est l'usage qu'on en fait qui compte, le fabricant du couteau n'est pas responsable d'un meurtre qu'on commet avec ce couteau, donc on ne doit pas se poser la question des droits humains ». Avant Snowden, c'était sans doute l'opinion dominante à l'IETF, mais cela a changé depuis.

Mais, au fait, ce sont quoi, les Droits Humains avec leur majuscule ? Ce sont des droits **universels**, **indivisibles** et **inaliénables**, formalisés dans des textes comme la Déclaration Universelle des Droits de l'Homme ou comme le pacte international relatif aux droits civils et politiques <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx> ou le Pacte international relatif aux droits économiques, sociaux et culturels <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>. La section 2 du RFC, sur la terminologie, discute en détail cette définition. Si vous voulez un document unique sur les droits humains, la DUDH citée plus haut est une lecture recommandée. Le fait qu'ils soient universels est important : on entend régulièrement des dirigeants ou des lécheurs de bottes des dirigeants prétendre que les droits humains ne sont pas bons pour le peuple qu'ils oppriment, qu'ils seraient uniquement pour certaines catégories de l'humanité. Si c'était le cas, il serait en effet inutile de discuter des droits humains sur l'Internet, puisque celui-ci connecte tout le monde. Mais, bien sûr, cette soi-disant relativité des droits humains est de la pure rhétorique malhonnête au service de dictateurs locaux.

On notera que, à l'époque de la rédaction de la DUDH, le seul risque de violation envisagée était l'œuvre des États, mais que l'idée s'est imposée depuis que des acteurs non-étatiques pouvaient également être concernés.

Cela ne veut pas dire que les textes comme la DUDH citée plus haut sont parfaits. Ce ne sont pas des textes sacrés, mais le résultat d'un processus politique. Comme toute œuvre humaine, ils peuvent être améliorés, mais il faut juste garder en tête que ceux qui les critiquent ne cherchent pas en général à les améliorer, mais à les affaiblir, voire à les détruire.

Par contre, les droits humains ne sont pas absolus. Un exemple de ce caractère non-absolu des droits humains est qu'ils peuvent être en conflit entre eux. Par exemple, le droit à la liberté d'expression peut rentrer en contradiction avec le droit de ne pas être insulté ou harcelé. Ou avec le droit à la vie privée. Les droits humains ne pourront donc pas être mis en algorithmes.

La section 2 de notre RFC est consacrée à la terminologie. Sujet très difficile car elle est souvent floue dans les domaines liés à la sécurité. Je ne vais pas la reproduire en entier ici (la section est longue, en partie en raison du caractère transversal de notre RFC, cf. section 5.2.1.3), juste noter quelques définitions qui ont fait des histoires (listées dans l'ordre alphabétique de l'original en anglais). Notez que notre RFC 8280 ne fait souvent que reprendre des définitions de RFC précédents. Ainsi, la définition de « connectivité Internet complète » vient du RFC 4084 (et est nécessaire car bien des malhonnêtes vendent comme « accès Internet » des offres plus ou moins bridées). De même le RFC 4949, sur le vocabulaire de la sécurité, et le RFC 6973, sur la vie privée, sont très mis à contribution.

En parlant de vie privée, la définition d'« anonymat » est un des premiers problèmes de terminologie. Le terme est utilisé à tort et à travers dans les médias (« Bitcoin est une monnaie anonyme ») et souvent confondu avec pseudonymat. À leur décharge, il faut dire que les définitions du RFC 4949 et du RFC 6973 sont très abstraites.

Parmi les autres définitions plutôt vagues, notons celle de « neutralité par rapport au contenu » ("*content agnosticism*"). C'est bien sûr un concept très important, d'autant plus que cette neutralité <https://www.bortzmeyer.org/neutralite.html> est menacée, mais la définition ne va pas très loin. Ce n'est pas mieux pour un autre concept important mais flou, et difficile à saisir, celui de décentralisation, un peu utilisé à toutes les sauces aujourd'hui (cf. mon article pour JRES <https://conf-ng.jres.org/2015/planning.html#article_52>).

Passons maintenant au principe de bout en bout. C'est un des concepts clés de l'Internet (RFC 2775) : l'« intelligence » (les traitements compliqués) doit être aux extrémités, pas dans le réseau. Plusieurs raisons militent en faveur de ce principe mais, pour en rester aux droits humains, notons surtout que ce principe se traduit par « touche pas à mes données ».

Autre sujet difficile à définir, les « normes ouvertes » ("*open standards*"). Il y a plein de SDO, dont le degré d'ouverture varie considérablement. Par exemple, l'ISO ou l'IEEE ne publient pas leurs normes en ligne et, même si on les acquiert, on n'a pas le droit de les redistribuer. L'UIT ne permet de participer que si vous êtes gouvernement ou grande entreprise. L'IETF, sans doute la SDO la plus ouverte, n'a pas de définition claire de ce qu'est une norme ouverte (cf. RFC 2026), à part dans le RFC 6852, qui est surtout un document politicien (et hypocrite).

Un concept important de l'Internet est celui d'« innovation sans autorisation ». Pour le comprendre, regardons l'invention du World-Wide Web. Tim Berners-Lee, Robert Cailliau et les autres ont pu inventer le Web et le déployer, sans rien demander à personne. Aucun comité Machin, aucun gouvernement, n'a été sollicité pour donner son avis ou son autorisation. Au contraire, dans les réseaux de télécommunication pré-Internet, il fallait l'accord préalable de l'opérateur pour tout déploiement d'une application. Sans l'« innovation sans autorisation », nous n'aurions pas le Web.

Et la « vie privée », on la définit comment ? Le RFC 4949 la définit comme le droit à contrôler ce qu'on expose à l'extérieur. C'est actuellement un des droits humains les plus menacés sur l'Internet, en raison des possibilités de surveillance massive que permet le numérique, possibilités largement utilisées par les États. Or, ce droit est lui-même à la base de nombreux autres droits. Ainsi, la liberté d'expression est sérieusement en danger si on n'a pas de droit à la vie privée, par exemple parce que des gens hésiteront à lire certains textes s'ils savent que leurs habitudes de lecture sont surveillées.

La section 4 du RFC est consacrée à un examen du débat (très ancien) sur la neutralité de la technique, et sur les relations entre technique et politique. La littérature scientifique et philosophique dans ce domaine est riche ! (À une réunion de HRPC, la discussion avait tourné à la pure philosophie, et on y avait abondemment cité Foucault, Heidegger, Wittgenstein, Derrida et Kant, ce qui est plutôt rare à l'IETF.)

Les deux opinions extrêmes à ce sujet sont :

— L'IETF fait un travail purement technique. Un protocole de communication est un outil, il est neutre, comme, mettons, une voiture, qui peut servir à des gens sympas à se déplacer, ou à des méchants pour commettre un crime.
— « Tout est politique », toute décision prise par des humains, humains insérés dans un environnement social réel, toute décision va forcément affecter la vie des autres (ou alors c'est que ces décisions n'ont servi à rien) et est donc politique. Pour citer J. Abbate <https://mitpress.mit.edu/books/inventing-internet>, « "*protocol is politics by other means*" ».

Il n'est pas compliqué de trouver plein d'exemples de luttes politiques autour des protocoles Internet, dans les RFC cités plus haut comme le RFC 7258, ou bien dans des articles comme celui de Denardis « "*The Internet Design Tension between Surveillance and Security*" <http://is.gd/7GAnFy> ». Les participants à l'IETF ne vivent pas dans une bulle, ils vivent dans un contexte politique, social, historique, culturel, et cela affecte certainement leurs décisions.

Notre RFC cite un grand nombre de publications sur ces sujets, de Francesca Musiani « "*Giants, Dwarfs and Decentralized Alternatives to Internet-based Services*" <https://www.westminsterpapers.org/articles/10.16997/wpcc.214/> » à Lawrence Lessig, Jonathan Zittrain (« "*The future of the Internet*" <https://www.bortzmeyer.org/future-internet.html> ») et Milton Mueller. Si vous avez quelques mois de libres devant vous, je vous encourage à lire tous ces livres et articles.

Il y a aussi des études plus spécifiques au rôle des SDO, parmi lesquelles « "*Engineering 'Privacy by Design' in the Internet Protocols - Understanding Online Privacy both as a Technical and a Human Rights Issue in the Face of Pervasive Monitoring*" <https://www.ietf.org/mail-archive/web/hrpc/current/pdfRBnRYFeVsm.pdf> » ou le célèbre article de Clark et ses collègues, « "*Tussle in Cyberspace*" <https://www.bortzmeyer.org/tussle-cyberspace.html> ».

Le RFC dégage cinq opinions différentes sur les relations entre le travail des ingénieurs et les droits humains, et sur la question de savoir si les droits humains doivent être intégrés dans les protocoles Internet. La première est celle citée dans l'article de Clark et al. <https://www.bortzmeyer.org/tussle-cyberspace.html>, qu'on peut résumer par « ce serait dangereux d'essayer de faire respecter les droits humains par les protocoles » :

— Les droits humains ne sont pas absolus, et un système technique ne peut pas comprendre cela.
— Il y a d'autres outils que les protocoles (l'action politique classique par exemple). C'était un peu l'opinion défendue avec fougue par Milton Mueller à la réunion HRPC <https://datatracker.ietf.org/meeting/99/materials/slides-99-hrpc-presentation-milton-mueller-requiem-for> lors de l'IETF 99 à Prague <https://www.ietf.org/meeting/99/index.html>.
— Il est mauvais de faire des promesses qu'on ne peut pas tenir. Par exemple, on ne peut pas espérer développer de systèmes cryptographiques invulnérables, et donc on ne doit pas compter uniquement sur eux.

L'article résume en disant que les ingénieurs doivent concevoir le terrain, pas le résultat du match.

Une deuxième position est que certaines valeurs universelles, dont les droits humains tels que formalisés dans la DUDH, devraient être incluses dans l'architecture même du réseau. (Cf. l'article « "*Should Specific Values Be Embedded In The Internet Architecture ?*" <http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf> », et attention, c'est un article collectif, avec plusieurs points de vue. Celui résumé ici est celui de Brown.) L'idéal serait que le réseau lui-même protège ces droits. En effet, les techniciens, de part le pouvoir qu'ils ont, ont une obligation « morale » de faire tout ce qui est possible pour faire respecter les droits humains.

Une troisième position, qui part sur un plan différent, est d'estimer qu'on ne peut pas inclure le respect des droits humains dans les protocoles, mais que c'est bien dommage et, qu'à défaut, il faudrait déclarer clairement que le réseau est un bien commun, et que toute tentative de l'utiliser pour le mal est en soi une violation des droits humains. Si on suit ces auteurs (« "*The public core of the Internet. An international agenda for Internet governance*" <https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet> »), l'Internet lui-même, et les protocoles tels que normalisés dans les RFC, seraient un bien commun qu'on ne peut pas tripoter, comme un parc naturel, par exemple. Si le DNS était inclus comme « bien commun », des manipulations comme les résolveurs menteurs <https://www.bortzmeyer.org/dns-menteur.html> deviendraient illégales ou en tout cas immorales.

Les auteurs de « "*Values and Networks*" <https://dl.acm.org/citation.cfm?id=2935640&dl=ACM&coll=DL&CFID=824161411&CFTOKEN=51249534> » sont plus prudents. Ils estiment que les protocoles Internet ont effectivement des conséquences sur les droits humains, mais qu'on n'est pas sûrs de quelles conséquences exactement, et qu'il est important de poursuivre les recherches. Cette quatrième position va donc tout à fait dans le sens de la constitution de HRPC <https://irtf.org/hrpc> comme groupe de recherche de l'IRTF.

Enfin, cinquième possibilité (et vous avez vu qu'elles ne sont pas forcément incompatibles), Berners-Lee et Halpin <http://www.ibiblio.org/hhalpin/homepage/publications/def-timbl-halpin.pdf> disent que l'Internet crée également de nouveaux droits. Ainsi, dans une société connectée où ne pas avoir l'Internet est un handicap social, le droit à un accès Internet devient un droit humain.

Quel bilan tirer de cette littérature scientifique et philosophique existante ? D'abord, d'un point de vue pratique, on ne sait pas si créer un réseau qui, par construction, assurerait le respect des droits humains est faisable (avant même de savoir si c'est souhaitable). Mais, au moins, on peut arrêter de croire que la technique est complètement neutre, étudier les conséquences des protocoles sur les droits humains (ce que fait la section 5 de notre RFC) et essayer d'améliorer ces protocoles à la lumière de cette analyse (la section 6 du RFC).

Voyons donc une série d'étude de cas de protocoles Internet existants, et en quoi ils affectent les droits humains (section 5). Une anecdote personnelle au passage : les premières versions de ces études de cas comportaient d'énormes erreurs techniques. Il est en effet difficile de trouver des gens qui sont à la fois sensibilisés aux droits humains **et** compétents techniquement. Comme le note le RFC, un travail interdisciplinaire est nécessaire. Le travail collectif à l'IRTF fait que cette section 5 est maintenant correcte.

Avant les études de cas techniques, le point de départ est une analyse des discours (selon la méthodologie présentée dans l'article de Cath <https://www.ietf.org/mail-archive/web/hrpc/current/pdf36GrmRM84S.pdf>). Elle s'est faite à la fois informellement (discussion avec des auteurs de RFC, interviews de participants à l'IETF) et formellement, par le biais d'un outil d'analyse automatique. Ce dernier, écrit en Python avec Big Bang <https://github.com/npdoty/rfc-analysis>, a permis de déterminer les « éléments de langage » importants dans les normes Internet. Et cela donne de jolis graphes <https://npdoty.name/rfc-analysis/graphs/>.

La partie informelle s'est surtout faite pendant la réunion IETF 92 <https://www.ietf.org/meeting/92/index.html> à Dallas, et a donné le film « "*Net of Rights*" <https://www.youtube.com/watch?v=m1U0Ebix-aQ> ». Mais il y a eu aussi l'observation des groupes de travail IETF en action.

Les protocoles Internet sont bâtis en utilisant des concepts techniques (connectivité, confidentialité, accessibilité, etc) et la section 5.2.2 met en correspondance ces concepts avec les droits humains tels que définis dans la DUDH. Par exemple, le droit de s'assembler s'appuie sur la connectivité, mais aussi sur la résistance à la censure, et sur la sécurité en général.

Maintenant, place à la première partie technique de notre RFC, la section 5.2.3. Elle étudie en détail les conséquences de divers protocoles pour les droits humains. Attention, la conception d'un protocole est une activité complexe, avec des cahiers de charges épais où le respect des droits humains (quand il est présent…) n'est qu'une partie. Et le travail d'ingéniérie nécessite toujours des compromis. Le RFC prévient donc que ce travail est forcément étroit : on n'examine les protocoles que sous l'angle des droits humains, alors qu'une évaluation complète de ces protocoles nécessiterait la prise en compte de bien d'autres aspects. Comme exemple de compromis auquel il faut parfois se résoudre, avoir un serveur

distinct de la machine de l'utilisat·eur·rice, possiblement géré par un tiers (c'est le cas de SMTP et XMPP), est certainement mauvais pour la résistance à la censure, car il va fournir un point de contrôle évident, sur lequel des autorités peuvent taper. D'un autre côté, sans un tel serveur, comment communiquerait-on avec des utilisat·eur·rice·s qui ne sont pas connecté·e·s en permanence ou qui sont coincé·e·s derrière un réseau qui interdit les connexions entrantes ? Bref, les protocoles qui sont souvent vertement critiqués par la suite ne sont pas forcément mauvais, encore moins délibérement mauvais. L'idée de cette section est de bien illustrer, sur des cas concrets, que les décisions techniques ont des conséquences politiques. (Ce point avait fait l'objet de vives discussions à l'IETF, des gens estimant que le RFC était trop négatif, et qu'il aurait également fallu indiquer les aspects positifs de l'Internet.)

Donc, pour commencer la série, évidemment, IP lui-même, plus précisement IPv4 (RFC 791). Malgré la normalisation d'IPv6, IPv4 est toujours le principal protocole du réseau. C'est un succès fou, connectant des centaines de millions de machines (et bien plus via les systèmes de traduction d'adresses). Il est conçu pour en faire le moins possible : l'intelligence doit être dans les machines terminales, pas dans le réseau, pas dans la couche 3. (Cf. RFC 3724.) En pratique, toutefois, on voit des intermédiaires agir au niveau IP et, par exemple, ralentir certains types de trafic, ou bien bloquer certaines machines. IP expose en effet certaines informations qui peuvent faciliter ce genre de violations de la neutralité du réseau.

Par exemple, les adresses IP source et destination sont visibles en clair (même si tout le reste du paquet est chiffré) et à un endroit fixe du paquet, ce qui facilite la tâche des routeurs mais aussi des dispositifs de blocage. Avant que vous ne me dites « ben, évidemment, sinon le réseau ne pourrait pas marcher », faites attention. L'adresse IP de destination est effectivement nécessaire aux routeurs pour prendre des décisions de transmission, mais ce n'est pas le cas de l'adresse source. En outre, IP expose le protocole de transport utilisé, encore une information dont les routeurs n'ont pas besoin, mais qui peut aider des intermédiaires à traiter certains types de trafic différemment.

Aujourd'hui, beaucoup de décisions de blocage sont prises sur la base des adresses IP ainsi exposées, ce qui illustre les conséquences d'une décision apparemment purement technique. (Pour les amateurs d'histoire alternative, X.25 n'exposait pas obligatoirement les adresses source et destination dans chaque paquet. Même le serveur final ne les voyait pas forcément. X.25 avait plein de défauts, mais cette anecdote montre que d'autres choix étaient possibles. Il faut juste se rappeler qu'ils avaient leurs propres inconvénients.) Si vous êtes enseignant·e en réseaux informatiques, voici un exercice intéressant faire faire à vos étudiant·e·s : « concevoir un réseau qui n'expose pas à tous des identificateurs uniques mondiaux ». Des alternatives au mécanisme d'IP ont été conçues (comme Hornet <https://dl.acm.org/citation.cfm?id=2813628> ou APIP <https://dl.acm.org/citation.cfm?id=2626306>) mais aucune n'a connu de déploiement significatif. Le routage par la source (combiné avec de la triche sur les adresses IP) aurait également permis de limiter l'exposition des adresses IP sur le trajet mais il pose bien d'autres problèmes. La principale solution employée aujourd'hui, lorsqu'on veut dissimuler les adresses IP des machines qui communiquent, est Tor.

Une autre particularité d'IPv4, qui n'était pas présente à ses débuts, est l'utilisation massive de la traduction d'adresses (RFC 3022). Elle est très répandue <http://www.icsi.berkeley.edu/pubs/networking/NATusage11.pdf>. Mais elle casse le modèle de bout en bout, et met le routeur qui fait la traduction dans une position privilégiée (par exemple, beaucoup refusent de faire passer d'autres protocoles de transport que TCP ou UDP). C'est donc une sérieuse limite à la connectivité et donc aux droits humains qui en dépendent.

Et le DNS ? Voilà un protocole dont la relation aux droits humains a été largement discutée. Comme toute opération sur l'Internet commence par une requête DNS, il est un point de contrôle évident. On peut notamment l'utiliser pour la censure <https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes>. Autre question politique liée au DNS et qui a fait s'agiter beaucoup d'électrons, le pouvoir des organismes qui gèrent les TLD et,

bien sûr, la racine du DNS. On peut dire sans exagérer que l'essentiel des débats sur la « gouvernance de l'Internet » ont tourné sur la gestion de la racine du DNS, qui ne représente pourtant pas, et de loin, le seul enjeu politique.

Pourquoi est-ce un enjeu pour les droits humains ? Le DNS a une structure arborescente, avec l'ICANN à la racine. Le contrôle de l'ICANN fait donc saliver bien du monde. Ensuite, les TLD, qu'ils soient contrôlés par l'ICANN (les gTLD) ou pas, ont un rôle politique important, via leur politique d'enregistrement. Celle-ci varie selon les TLD. Les gTLD historiques comme `.com` ont une politique déterminée par des organisations états-uniennes, l'ICANN et leur registre (Verisign dans le cas de `.com`). Les nouveaux gTLD ont des registres de nationalité différentes mais dépendent tous des règles ICANN (cf. l'excellente étude de l'EFF comparant ces politiques dans l'optique des droits humains <https://www.eff.org/wp/which-internet-registries-offer-best-protection-domain-owners>). Les ccTLD, eux, dépendent de lois nationales très variables. Elles sont par exemple plus ou moins protectrices de la liberté d'expression. (Voir le fameux cas lybien <http://techyum.com/2010/10/official-vb-ly-link-short>.)

Est-ce que les centaines de nouveaux gTLD <https://www.bortzmeyer.org/gtld-json.html> créés depuis quelques années ont amélioré les choses ou pas, pour cette liberté d'expression ? Certains disent que non car beaucoup de ces nouveaux TLD ont une politique d'enregistrement restrictive (cf. le rapport de l'EFF cité plus haut), d'autres disent que oui car ces nouveaux TLD ont élargi le choix. Et que la liberté d'association peut ne pas bien s'entendre avec la liberté d'expression (la première peut justifier des règles restrictives, pour que des minorités discriminées puissent se rassembler sans être harcelées). Une chose est sûre, les débats ont été chauds, par exemple autour d'une éventuelle création du `.gay` (un rapport du Conseil de l'Europe <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b5a14> détaille cette question « TLD et droits humains »).

Le DNS soulève plein d'autres questions liées aux droits humains. Par exemple, il est indiscret (RFC 7626), et des solutions partielles comme le RFC 9156 semblent très peu déployées.

Et, comme trop peu de zones DNS sont protégées par DNSSEC (et, de toute façon, DNSSEC ne protège pas contre toutes les manipulations), il est trop facile de modifier les réponses envoyées. C'est aujourd'hui une des techniques de censure les plus déployées, notamment en Europe (voir à ce sujet le très bon rapport du Conseil Scientifique de l'AFNIC <https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-s.html>). Parmi les moyens possibles pour censurer via les noms de domaine :

— Faire supprimer le nom auprès du registre ou du BE, comme dans les saisies faites par l'ICE, ou comme dans le cas de Wikileaks <http://news.bbc.co.uk/2/hi/technology/7250916.stm>. Le protocole ne permet pas de faire la différence entre une saisie au registre, et une réelle suppression. Des systèmes comme Namecoin fournissent une meilleure protection (mais ont leurs propres défauts <https://www.bortzmeyer.org/maman-j-ai-perdu-mon-namecoin.html>).
— Si on ne peut pas peser sur le registre ou sur le BE, on peut agir lors de la résolution du nom, avec des résolveurs menteurs <https://www.bortzmeyer.org/censure-francaise.html> ou bien carrément des modifications faites dans le réseau, méthode surtout connue en Chine <https://www.bortzmeyer.org/detournement-racine-pekin.html>, mais également en Grèce <https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-upda.pdf>. La première technique, le résolveur menteur, peut être défaite par un changement de résolveur (ce qui peut créer d'autres problèmes <https://www.bortzmeyer.org/dns-resolveurs-publ.html>), la seconde attaque nécessite des solutions comme le RFC 7858.

Le RFC étudie ensuite le cas de HTTP, le protocole vedette de l'Internet (RFC 7230 et suivants). Sa simplicité et son efficacité ont largement contribué à son immense succès, qui a à son tour entrainé celui de l'Internet tout entier. On voit même aujourd'hui des tas de services non-Web utiliser HTTP comme substrat. Du fait de cette utilisation massive, les conséquences des caractéristiques de HTTP pour les droits humains ont été beaucoup plus étudiées que le cas du DNS.

Premier problème, HTTP est par défaut peu sûr, avec des communications en clair, écoutables et modifiables. Si la solution HTTPS est très ancienne (le RFC 2828 a dix-sept ans…, et SSL avait été décrit et mis en œuvre avant), elle n'a été massivement déployée que depuis peu, essentiellement grâce au courage d'Edward Snowden.

En attendant ce déploiement massif de HTTPS, d'innombrables équipements réseau de censure et de détournement de HTTP ont été fabriqués et vendus (par exemple par Blue Coat mais ils sont loin d'être les seuls <https://surveillance.rsf.org/>). Celui qui veut aujourd'hui empêcher ou perturber les communications par HTTP n'a pas besoin de compétences techniques, les solutions toutes prêtes existent sur le marché.

Un autre RFC qui touchait directement aux droits humains et qui avait fait pas mal de bruit à l'IETF est le RFC 7725, qui normalise le code d'erreur 451, renvoyé au client lorsque le contenu est censuré. Il permet une « franchise de la censure », où celle-ci est explicitement assumée.

Les discussions à l'IETF avaient été chaudes en partie parce que l'impact politique de ce RFC est évident, et en partie parce qu'il y avait des doutes sur son utilité pratique. Beaucoup de censeurs ne l'utiliseront pas, c'est clair, soit parce qu'ils sont hypocrites, soit parce que les techniques de censure utilisées ne reposent pas sur HTTP mais, par exemple, sur un filtrage IP. Et, lorsque certains l'utilisent, quelle utilité pour les programmes ? Notre RFC explique que le principal intérêt est l'étude du déploiement de la « censure honnête » (ou « censure franche »). C'est le cas de projets comme Lumen <https://lumendatabase.org/>. Du code est d'ailleurs en cours de développement pour les analyses automatiques des 451 (on travaillera là-dessus au hackathon de la prochaine réunion IETF <https://www.ietf.org/registration/MeetingWiki/wiki/100hackathon>).

Outre la censure, l'envoi du trafic en clair permet la surveillance massive, par exemple par les programmes Tempora ou XKeyscore. Cette vulnérabilité était connue depuis longtemps mais, avant les révélations de Snowden, la possibilité d'une telle surveillance de masse par des pays supposés démocratiques était balayée d'un revers de main comme « paranoïa complotiste ». Pour la France, souvenons-nous qu'une société française vend des produits d'espionnage de leur population à des dictatures, comme celle du défunt Khadafi <http://www.wsj.com/articles/SB10001424053111904199404576538720773970988>.

D'autre part, l'attaque active, la modification des données en transit, ne sert pas qu'à la censure. Du trafic HTTP changé en route peut être utilisé pour distribuer un contenu malveillant (possibilité utilisée dans QUANTUMINSERT/FOXACID) ou pour modifier du code envoyé lors d'une phase de mise à jour du logiciel d'une machine. Cela semble une attaque compliquée à réaliser ? Ne vous inquiétez pas, jeune dictateur, des sociétés vous vendent ce genre de produits <https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/> clés en main.

HTTPS n'est évidemment pas une solution magique, qui assurerait la protection des droits humains à elle seule. Pour ne citer que ses limites techniques, sa technologie sous-jacente, TLS (RFC 5246) a été victime de plusieurs failles de sécurité (sans compter les afaiblissements délibérés comme les célèbres « algorithmes pour l'exportation »). Ensuite, dans certains cas <https://moxie.org/software/sslstrip/>, un·e utilisat·eur·rice peut être incité·e à utiliser la version en clair (attaque par repli, contre laquelle des techniques comme celles du RFC 6797 ont été mises au point).

HTTPS n'étant pas obligatoire, la possibilité d'une attaque par repli existe toujours. Pour HTTP/2, il avait été envisagé d'imposer HTTPS, pour qu'il n'y ait plus de version non sûre, mais le RFC 7540 n'a finalement pas entériné cette idée (que le RFC 8164 a partiellement ressorti depuis.)

Autre protocole étudié, XMPP (RFC 6120). Un de ses principes est que le logiciel client (par exemple pidgin) ne parle pas directement au logiciel du correspondant, mais passe forcément par un (ou deux) serveur(s). Cette architecture présente des avantages pratiques (si le correspondant est absent, son serveur peut indiquer cette absence à l'appelant) mais aussi en matière de protection (on ne voit pas l'adresse IP de l'appelant). Ces serveurs sont fédérés entre eux, XMPP, contrairement à des protocoles inférieurs comme Slack ne peut donc pas être arrêté par décision supérieure.

Mais XMPP a aussi des inconvénients. Les utilisat·eurs·rices sont identifiés par un JID comme `bortzmeyer@examp` qui comprend une « ressource » (le terme après la barre oblique) qui, en pratique, identifie souvent une machine particulière ou un lieu particulier. En général, ce JID est présenté tel quel aux correspondants, ce qui n'est pas idéal pour la vie privée. D'autre part, les communications sont en clair par défaut, mais peuvent être chiffrées, avec TLS. Sauf que l'utilisat·eur·rice ne sait pas si son serveur chiffre avec le serveur suivant, ou bien le serveur final avec son correspondant. Sans possibilité d'évaluation de la sécurité, il faut donc faire une confiance aveugle à tous les serveurs pour prendre des précautions. Et espérer qu'ils suivront tous le « "*XMPP manifesto*" <`https://raw.githubusercontent.com/stpeter/manifesto/master/manifesto.txt`> ».

Si XMPP lui-même est fédéré et donc relativement résistant à la censure, les salles collectives de discussion sont centralisées. Chaque salle est sur un serveur particulier, une sorte de « propriétaire », qui peut donc contrôler l'activité collective, même si aucun des participants n'a de compte sur ce serveur. (En prime, ces salles sont une extension du protocole, spécifiée dans le XEP-0045 <`https://xmpp.org/extensions/xep-0045.html`>, pas mise en œuvre de manière identique partout, ce qui est un problème non-politique fréquent avec XMPP.)

Et le pair-à-pair, lui, quelles sont ses implications pour les droits humains ? D'abord, il faut évidemment noter que ce terme ne désigne pas un protocole particulier, qu'on pourrait analyser en détail, mais une famille de protocoles très divers (RFC 5694). L'application la plus connue du pair-à-pair est évidemment l'échange de fichiers culturels, mais le pair-à-pair est une architecture très générale, qui peut servir à plein de choses (Bitcoin, par exemple).

À l'époque des GAFA, monstres centralisés qui contrôlent toutes les interactions entre utilisat·eur·rice·s, le pair-à-pair est souvent présenté comme la solution idéale à tous les problèmes, notamment à la censure. Mais la situation est plus compliquée que cela.

D'abord, les réseaux en pair-à-pair, n'ayant pas d'autorité centrale de certification des contenus, sont vulnérables aux diverses formes d'empoisonnement des données. On se souvient des faux MP3 sur eDonkey, avec un nom prometteur et un contenu décevant. Un attaquant peut aussi relativement facilement corrompre, sinon les données, en tout cas le routage qui y mène.

Comme les protocoles pair-à-pair représentent une bonne part du trafic Internet <`https://www.sandvine.com/pr/2015/12/7/sandvine-over-70-of-north-american-traffic-is-now-streaming-html`>, et qu'ils sont souvent identifiables sur le réseau, le FAI peut être tenté de limiter leur trafic <`https://torrentfreak.com/is-your-isp-messing-with-bittorrent-traffic-find-out-140123`>.

Plus gênant, question droits humains, bien des protocoles pair-à-pair ne dissimulent pas l'adresse IP des utilisat·eur·rice·s. En BitTorrent, si vous trouvez un pair qui a le fichier qui vous intéresse, et que

vous le contactez, ce pair apprendra votre adresse IP. Cela peut servir de base pour des lettres de menace <https://torrentfreak.com/lawyers-sent-109000-piracy-threats-in-germany-during-2013-140304/> ou pour des poursuites judiciaires (comme avec la HADOPI en France). Il existe des réseaux pair-à-pair qui déploient des techniques de protection contre cette fuite d'informations personnelles. Le plus ancien est Freenet mais il y a aussi Bitmessage <https://www.bortzmeyer.org/bitmessage.html>. Ils restent peu utilisés.

Autre danger spécifique aux réseaux pair-à-pair, les attaques Sybil. En l'absence d'une vérification que l'identité est liée à quelque chose de coûteux et/ou difficile à obtenir, rien n'empêche un attaquant de se créer des millions d'identités et de subvertir ainsi des systèmes de vote. L'attaque Sybil permet de « bourrer les urnes » virtuelles. (Ne ratez pas l'article de Wikipédia sur l'"*astroturfing*".)

C'est pour lutter contre cette attaque que Bitcoin utilise la preuve de travail et que CAcert utilise des certifications faites pendant des rencontres physiques, avec vérification de l'identité étatique. Le RFC note qu'on n'a pas actuellement de solution générale au problèmes des attaques Sybil, si on exige de cette solution qu'elle soit écologiquement durable (ce que n'est pas la preuve de travail) et entièrement pair-à-pair (ce que ne sont pas les systèmes d'enrôlement typiques, où un acteur privilégié vérifie les participants à l'entrée). Quant aux solutions à base de « réseaux de connaissances » (utilisées dans le "*Web of Trust*" de PGP), elles sont mauvaises pour la vie privée, puisqu'elles exposent le graphe social des participants.

Bref, le pair-à-pair n'est pas actuellement la solution idéale à tous les problèmes de droits humains, et les recherches doivent se poursuivre.

Un autre outil est souvent présenté comme solution pour bien des problèmes de respect des droits humains, notamment pour la sécurité de ceux qui vivent et travaillent dans des pays dictatoriaux, le VPN. On entend parfois des discussions entre militants des droits humains, ou bien entre journalistes, sur les avantages comparés de Tor et du VPN pour regarder le Web en toute sécurité. En fait, les deux ne fournissent pas réellement le même service et, pire, les propriétés du VPN sont souvent mal comprises. Le VPN fonctionne en établissant une liaison sécurisée (authentifiée, chiffrée) avec un fournisseur, qui va ensuite vous connecter à l'Internet. Il existe plusieurs systèmes techniques ouverts pour cela (IPsec, OpenVPN) mais la question centrale et difficile est le choix du fournisseur. Les VPN sont très populaires, et il existe donc une offre commerciale abondante. Mais, en général, il est impossible d'évaluer sa qualité, aussi bien technique (même si le protocole est standard, le fournisseur impose souvent un logiciel client à lui, binaire non auditable, et des failles ont déjà été découvertes dans certains VPN) que politique (ce fournisseur de VPN qui dit ne pas garder de journaux dit-il la vérité ?) On est très loin de l'attention qui a été portée à la sécurité de Tor, et des innombrables évaluations et analyses dont Tor a fait l'objet !

Il existe aussi des attaques plus sophistiquées (et pas à la portée de la première police venue) comme la corrélation de trafic (entre ce qui entre dans le VPN et ce qui en sort) si l'attaquant peut observer plusieurs points du réseau (la NSA le fait <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>).

Donc, un rappel à tou·te·s les utilisat·eur·rices·s de VPN : la question la plus importante est celle de votre fournisseur. Le VPN peut vous promettre l'anonymat, vous ne serez pas pour autant anonyme vis-à-vis de votre fournisseur. Celui-ci peut vous trahir ou, tout simplement, comme il est situé dans un pays physique, être forcé par les autorités de ce pays de vous dénoncer.

Une question bien plus délicate avait fait l'objet de nombreux débats à l'IETF, celle d'une possibilité de considérer certaines attaques dDoS comme « légitimes ». C'est par exemple un point de vue qui a été défendu par Richard Stallman <https://www.theguardian.com/commentisfree/2010/

dec/17/anonymous-wikileaks-protest-amazon-mastercard>. La position classique de l'IETF est qu'au contraire toutes les attaques dDoS sont négatives, impactant l'infrastructure (y compris des tas d'innocents) et sont au bout du compte une attaque contre la liberté d'expression. En simplifiant, il existe trois types d'attaques dDoS, les volumétriques (on envoie le plus de paquets ou d'octets possibles, espérant épuiser les ressources du réseau), les attaques sur les protocoles intermédiaires (comme les "*SYN flood*" ou comme le très mal nommé "*ping of death*"), attaques qui permettent à l'assaillant de n'envoyer que peu de paquets/octets, et enfin les attaques applicatives, visant les failles d'une application. Une attaque faite par LOIC tient de l'attaque volumétrique (on envoie le plus de requêtes HTTP possibles) et de l'attaque applicative, puisqu'elle ne fonctionne que parce que l'application n'arrive pas à suivre (sur la plupart des sites Web, où il faut exécuter des milliers de lignes de code PHP ou Java pour afficher la moindre page, l'application craque avant le réseau).

Dans les trois cas, cette possibilité d'attaque est avant tout une menace contre les médias indépendants, contre les petites associations ou les individus qui ne peuvent pas ou ne veulent pas payer la « protection » (le mot a un double sens en anglais...) des sociétés spécialisées. Et les attaques dDoS peuvent faciliter la tâche des censeurs hypocrites : il suffit de déguiser une censure en une attaque par déni de service. Une des principales raisons pour lesquelles on ne peut pas comparer l'attaque dDoS à une manifestation est que, dans une attaque dDoS, la plupart des participants ne sont pas volontaires, ce sont des zombies. Lorsque des gens manifestent dans la rue, ils donnent de leur temps, et parfois prennent des risques personnels. Lorsqu'une organisation puissante loue les services d'un botnet pour faire taire par dDoS un gêneur, elle ne dépense qu'un peu d'argent.

Il y a bien sûr quelques exceptions (l'opération Abibil <http://ddanchev.blogspot.be/2012/09/dissecting-operation-ababil-osint.html> ou bien le "*Green Movement*" <https://www.nartv.org/2009/06/16/iran-ddos/>) mais elles sont rares. Il est donc parfaitement justifié que l'IETF fasse tout son possible pour rendre les attaques dDoS plus difficiles (RFC 3552, section 4.6). Dans la discussion menant à ce nouveau RFC 8280, certaines voix se sont élevées pour demander qu'on puisse lutter seulement contre les « mauvaises » dDoS. Mais c'est aussi absurde que l'idée récurrente des ministres de faire de la cryptographie « légale » qui ne pourrait protéger que les gens honnêtes !

Nous en arrivons maintenant à la partie la plus utilitaire de ce RFC, la section 6, qui est la méthodologie qui devrait être suivie lors du développement d'un nouveau protocole, pour comprendre son impact sur les droits humains, et pour essayer de minimiser les conséquences négatives, et maximiser les positives. Cette section 6 (depuis largement remplacée par le RFC 9620) concerne donc surtout les développeurs de protocole, par exemple les auteurs des RFC techniques. (C'est pour cela que le début de la section 6 répète beaucoup de choses dites avant : on pense que pas mal de techniciens ne liront que cette section.) Évidemment, les conséquences (bonnes ou mauvaises) d'un protocole, ne sont pas uniquement dans la norme technique qui le définit. La façon dont le protocole est mis en œuvre et déployé joue un rôle crucial. (Par exemple, la domination excessive de Gmail n'est pas inscrite dans le RFC 5321.)

Un bon exemple d'une telle démarche est donnée par le RFC 6973, sur la protection de la vie privée. La première responsabilité du développeur de protocole est d'examiner les menaces sur les droits humains que ce protocole peut créer ou aggraver. De même qu'il est recommandé de réfléchir aux conséquences d'un nouveau protocole pour la sécurité de l'Internet (RFC 3552), et sur les conditions dans lesquelles ce protocole est utile, de même il faut désormais réfléchir aux conséquences de son protocole sur les droits humains. Notons que notre RFC ne dit pas « voici ce qu'il faut faire pour respecter les droits humains ». Cela serait clairement irréaliste, vu la variété des menaces et la diversité des protocoles. Notre RFC demande qu'on se pose des questions, il ne fournit pas les réponses. Et il n'impose pas d'avoir dans chaque RFC une section « "*Human Rights Considerations*" » comme il existe une « "*Security Considerations*" » obligatoire.

Bon, maintenant, la liste des choses à vérifier quand vous concevez un nouveau protocole (section 6.2). À chaque fois, il y a une ou plusieurs questions, une explication, un exemple et une liste d'impacts.

Par exemple, pour la question de la connectivité, les questions sont « Est-ce que votre protocole nécessite des machines intermédiaires ? Est-ce que ça ne pourrait pas être fait de bout en bout, plutôt ? Est-ce que votre protocole marchera également sur des liens à faible capacité <https://www.bortzmeyer.org/capacite.html> et forte latence <https://www.bortzmeyer.org/latence.html> ? Est-ce que votre protocole est à état (alors que les protocoles sans état sont souvent plus robustes) ? » L'explication consiste surtout à répéter l'intérêt des systèmes de bout en bout (RFC 1958). L'exemple est évidemment celui des conséquences négatives des "*middleboxes*". Et les impacts sont les conséquences sur la liberté d'expression et la liberté d'association. Bien sûr, tous les protocoles IETF se préoccupent peu ou prou de connectivité, mais ce n'était pas considéré jusqu'à présent comme pouvant impacter les droits humains.

Sur le deuxième point à vérifier, la vie privée, notre RFC renvoie au RFC 6973, qui demandait déjà aux auteurs de protocoles de faire attention à ce point.

Le troisième point est celui de la neutralité vis-à-vis du contenu. Il reste un peu vague, il n'y a pas actuellement d'exemple de protocole IETF qui soit activement discriminant vis-à-vis du contenu.

Quatrième point qui nécessite l'attention du développeur de protocole, la sécurité. Il est déjà largement traité dans de nombreux autres RFC (notamment le RFC 3552), il faut juste rappeler que ce point a des conséquences en matières de droits humains. Si un protocole a une faille de sécurité, cela peut signifier l'emprisonnement, la torture ou la mort pour un dissident.

En prime, le RFC rappelle que, contrairement à une utilisation réthorique fréquente, il n'y a pas **une** sécurité mais **plusieurs** services de sécurité. (Et certaines de ses propriétés peuvent avoir des frictions, par exemple la disponibilité et la confidentialité ne s'entendent pas toujours bien.)

Cinquième point que le développeur de protocoles doit vérifier, l'internationalisation (voir aussi le douzième point, sur la localisation). Eh oui, restreindre l'utilisation de l'Internet à ceux qui sont parfaitement à l'aise en anglais n'irait pas vraiment dans le sens des droits humains, notamment des droits à participer à la vie politique et sociale. D'où les questions « Est-ce que votre protocole gère des chaînes de caractères qui seront affichées aux humains ? Si oui, sont-elles en Unicode ? Au passage, avez-vous regardé le RFC 6365 ? » Dans le contexte IETF (qui s'occupe de protocoles et pas d'interfaces utilisateur), l'essentiel du travail d'internationalisation consiste à permettre de l'Unicode partout. Partout ? Non, c'est un peu plus compliqué que cela car l'IETF distingue les textes prévus pour les utilisat·eur·rice·s de ceux prévus pour les programmes (RFC 2277). Seuls les premiers doivent absolument permettre Unicode. (Cette distinction ne marche pas très bien pour les identificateurs, qui sont prévus à la fois pour les utilisat·eur·rice·s et pour les programmes, c'est le cas par exemple des noms de domaine.)

En prime, petite difficulté technique, il ne suffit pas d'accepter Unicode, il faut encore, si on accepte d'autres jeux de caractères et/ou encodages, l'indiquer (par exemple le `charset=` de MIME), sinon on risque le mojibake. Ou alors, si on n'accepte qu'un seul jeu de caractères / encodage, ce doit être UTF-8.

Sixième point sur la liste, une question dont les conséquences pour les droits humaines sont évidentes, la résistance à la censure. « Est-ce que votre protocole utilise des identificateurs qui peuvent être associés à des personnes ou à un contenu spécifique ? Est-ce que la censure peut être explicite ? Est-ce que la censure est facile avec votre protocole ? Si oui, ne pourrait-on pas le durcir pour la rendre plus difficile ? »

Un exemple est bien sûr la longue discussion du passé au sujet d'une méthode de fabrication des adresses IPv6. Le mécanisme recommandé à l'origine mettait l'adresse MAC dans l'adresse IP. Outre l'atteinte à la vie privée, cela facilitait la censure, permettant de bloquer un contenu pour seulement certaines personnes. (Ce mécanisme a été abandonné il y a longtemps, cf. RFC 4941.) Quand au cas de rendre la censure explicite, c'est une référence au code 451 (RFC 7725).

Septième point, les « normes ouvertes ». Intuitivement, il est évident qu'il vaut mieux des normes ouvertes que fermées. Mais attention, il n'existe pas de définition claire et largement adoptée, même pas à l'intérieur de l'IETF (qui est certainement une organisation très ouverte). Les questions posées dans ce RFC 8280 donnent une idée des critères qui peuvent permettre de décider si une norme est ouverte ou pas : « Le protocole est-il documenté publiquement ? Sa mise en œuvre peut-elle être faite sans code privateur ? Le protocole dépend t-il d'une technologie contrôlée par une entreprise particulière ? Y a-t-il des brevets (RFC 3979 et RFC 6701) ? »

Ce sont les normes ouvertes de la famille TCP/IP qui ont permis le développement et le déploiement massif de l'Internet. Les appropriations intellectuelles comme le secret industriel ou comme les brevets auraient tué l'Internet dans l'œuf. Il est donc logique que l'IETF soit une organisation particulièrement ouverte : les RFC sont publics et librement redistribuables, bien sûr (ce qui n'est pas le cas des normes d'autres SDO comme l'AFNOR, l'ISO ou l'IEEE), mais l'IETF publie également ses documents temporaires, ses listes de diffusion et ses réunions (ce que ne fait pas, par exemple, l'UIT).

(On note que le RFC 6852 traite également cette question mais c'est un document purement tactique, qui fait du « "*open washing*" » en faisant comme si l'IEEE était ouverte.)

Je saute le point huit, sur l'acceptation de l'hétérogénéité du réseau, et j'en arrive à l'important point neuf, sur l'anonymat. Le terme est très galvaudé (« Bitcoin est une monnaie anonyme » et autres erreurs). Il est souvent utilisé par les non-spécialistes comme synonyme de « une autre identité que celle de l'état civil » (ce qui est en fait la définition du pseudonyme, traité au point suivant). Normalement, même si la définition du RFC 4949 est très peu claire, l'anonymat implique la non-traçabilité : si un système est réellement anonyme, il ne doit pas être possible d'attribuer deux actions à la même entité.

Autre erreur courante quand on parle d'anonymat, la considérer comme une propriété binaire. C'est ce qui est fait quand un responsable ignorant affirme « les données sont anonymisées » (cela doit en général déclencher un signal d'alarme). En effet, il existe de nombreuses techniques, et en progrès rapide, pour « désanonymiser », c'est-à-dire pour relier des actions qui ne l'étaient a priori pas.

Cette confusion est d'autant plus dommage que l'anonymat est une propriété essentielle pour la sécurité du citoyen dans un monde numérique. Autrefois, la plupart des actions qu'on faisait dans la journée étaient anonymes, au sens où un observateur extérieur ne pouvait pas facilement les relier entre elles. Aujourd'hui, si vous mettez une photo sur Instagram, achetez un livre sur Amazon, et écrivez un document sur Google Docs, toutes ces actions sont facilement reliables entre elles, même si vos comptes se nomment respectivement « titi75 », « jean.durand » et « le_type_du_coin ». Par défaut, dans le monde numérique, tout est traçable, et il faut déployer des technologies compliquées pour retrouver un peu d'obscurité. En tout cas, rappelez-vous que l'anonymat n'est jamais parfait : c'est un but souhaitable, mais pas forcément atteignable.

Par exemple, la présence de votre adresse IP dans chaque paquet est un moyen simple de relier toutes vos activités (il en existe d'autres). Il est donc tout à fait légitime que l'adresse IP soit regardée comme une donnée personnelle <https://www.cnil.fr/fr/ladresse-ip-est-une-donnee-caractere-personn

Le pseudonymat, dixième point, est une propriété moins forte. C'est simplement le fait d'utiliser une identité persistante qui n'est pas l'identité officielle. On va utiliser un pseudonyme quand on veut masquer son orientation sexuelle, ou sa transidentité, ou l'entreprise où on travaille, mais tout en gardant une identité constante, par exemple pour avoir une réputation en ligne. C'est souvent une protection nécessaire contre le harcèlement <http://geekfeminism.wikia.com/wiki/Pseudonymity>, dont les femmes sont particulièrement fréquemment victimes en ligne. Outre les pseudonymes qu'on choisit, la nature du monde numérique fait que plein d'identificateurs attribués automatiquement sont des

pseudonymes. Ainsi, une adresse IP est un pseudonyme (elle cesse de l'être dès que votre FAI communique le nom et l'adresse de l'abonné aux autorités). Une adresse Bitcoin est un pseudonyme (Bitcoin est très traçable, c'est nécessaire pour son fonctionnement).

L'auteur·e de protocoles doit donc se méfier des informations qu'ielle expose. Si elles permettent de retrouver la personne à l'origine de la communication, ce sont des données personnelles. Par exemple, si vous exportez des données contenant des adresses IP (exemples en RFC 7011 ou bien pour les journaux d'un serveur), une des façons de brouiller la traçabilité (et donc de passer du pseudonymat à un relatif anonymat) est de ne garder qu'un préfixe assez général. Condenser les adresses IP n'est pas très efficace, un attaquant, un « désanonymiseur » peut condenser toutes les adresses possibles et ainsi retrouver l'information. D'une manière générale, soyez modeste : réellement anonymiser est très difficile.

Le onzième point concerne un sujet dont les conséquences en matière de droits humains sont claires pour quiconque a suivi les conférences Paris Web : l'accessibilité à tou·te·s, y compris en cas de handicap. L'accessibilité est une propriété nécessaire pour faire respecter le droit à ne pas être victime de discrimination. Cela ne concerne a priori pas l'IETF, qui ne fait pas d'interface utilisateur, mais c'est utile pour d'autres SDO. Ainsi, le RFC donne l'exemple de HTML, où l'obligation de mettre un attribut `alt` pour les images, oblige à réfléchir à l'accessibilité de la page Web aux malvoyants.

Le treizième point porte sur un concept très flou et d'autant plus répété qu'il n'a pas de définition claire : la « décentralisation ». Mon article à JRES sur ce sujet <`https://conf-ng.jres.org/2015/planning.html#article_52`> donne une idée de la complexité de la question. Le RFC traite la question par plusieurs questions : « Est-ce que le protocole a un point de contrôle unique ? Est-ce que le protocole ne pourrait pas être fédéré plutôt ? » Ça reste à mon avis trop vague mais, au moins, ça pousse les concepteurs de protocoles à réfléchir. La plupart des protocoles de base de l'Internet sont décentralisés ou fédérés comme vous voulez (et c'est explicitement souhaité par le RFC 3935), mais les services à la mode sont en général centralisés. (XMPP est fédéré mais dans les startups, on est obligés d'utiliser Slack qui est centralisé.)

Passons sur le point 14, la fiabilité (c'est sûr qu'un réseau qui marche, c'est mieux) et voyons le point 15, la confidentialité. Son impact sur les droits humains est clair : si des gens peuvent lire ma correspondance privée, mes droits sont clairement violés. La solution technique la plus évidente est le chiffrement et, aujourd'hui, le RFC 8280 estime à juste titre qu'un protocole sans possibilité de chiffrement (par exemple RFC 3912) est à éviter (RFC 3365). Et, même si le RFC ne le dit pas explicitement, il doit évidemment choisir d'un chiffrement sérieux, donc sans portes dérobées, sans affaiblissement délibéré.

Rédigé il y a trop longtemps, cette section dit que le DNS ne dispose pas de cette possibilité de chiffrement, mais c'est faux, depuis le RFC 7858.

Le RFC note à juste titre que le chiffrement ne protège pas contre les intermédiaires légitimes, comme dans l'exemple de XMPP cité plus haut : le chiffrement entre le client et le premier serveur XMPP ne protège pas contre ce serveur, qui voit tout passer en clair. Mais le RFC oublie de dire qu'il y a également le problème des extrémités : faire du HTTPS avec Gmail ne vous protège pas contre PRISM. Il faut donc également prévoir de la minimisation (envoyer le moins de données possible) pas seulement du chiffrement.

Je saute les points 16 (intégrité), 17 (authentification) et 18 (adaptabilité), je vous laisse les lire dans le RFC. Le dernier point, le dix-neuvième, porte sur la transparence : les utilisat·eur·rice·s peuvent-il·elle·s voir comment fonctionne le protocole et notamment quels sont les acteurs impliqués ? Par exemple, un service qui semble « gratuit » peut l'être parce qu'il y a derrière une grosse activité économique, avec de la publicité ciblée en exploitant vos données personnelles. Bref, si c'est gratuit, c'est peut-être que **vous** êtes le produit. Et vous ne le voyez peut-être pas clairement.

Voilà, si vous voulez en savoir plus, le RFC a une colossale bibliographie. Bonne lecture. Si vous préférez les vidéos, il y a mon intervention à Radio-France <`https://www.bortzmeyer.org/radiofrance-internet.html`> sur ce sujet.
