

REVUE STRATEGIQUE 2015 DE L'ARCEP

*Contribution des Master 2 Droit des Activités Spatiales et des Télécommunications et Droit
de l'Innovation et de la Propriété Industrielle de l'Université Paris XI Faculté Jean
Monnet*

Réponse à la question n°5

Rédacteurs de la contribution par les étudiants du M2 DAST¹ :

- Kahina BOUATOU
- Oriane FERREIRA
- Abdoul HAZIZ OUATTARA

Avec la collaboration des étudiants du M2 DIPI² :

- Anthony DORISON
- Arthur OMEZ

Coordination par Maître Olivier ITEANU, chargé d'enseignement en droit des communications électroniques internes des M2 DAST et DIPI

¹ Master 2 dirigé par Monsieur le Professeur Philippe Achilleas

² Master 2 dirigé par Monsieur le Doyen Antoine Latreille

Table des matières

Table des matières	3
1. La question : garantir la fiabilité des réseaux	4
2. La réponse	6
2.1. Importance de la fiabilité des réseaux	6
2.2. Organisation de l'obligation de notification des défaillances de réseaux.....	8
2.3. Publication des défaillances de réseaux	10
En conclusion et en synthèse.....	12

1. La question : garantir la fiabilité des réseaux

L'importance croissante du numérique rend les citoyens, les entreprises et les administrations de plus en plus dépendants de la fiabilité des réseaux. On parle de « résilience » pour caractériser la capacité d'une architecture à continuer de fonctionner en cas d'événement exceptionnel (pic ponctuel de surconsommation, panne ou cyberattaque). Un objectif important est de mieux articuler les enjeux de sécurité numérique (qui relève en premier lieu de l'Agence nationale de la sécurité des systèmes d'information – ANSSI) et de résilience générale des infrastructures (au-delà de la seule sécurité numérique). De plus, cette problématique de résilience des réseaux va aller en se complexifiant dans les réseaux fixes. En effet, alors que les boucles locales étaient historiquement détenues par un nombre restreint d'opérateurs, il sera désormais nécessaire de prendre en compte la multiplicité d'acteurs impliqués dans le déploiement de boucles locales optiques, chacun d'eux étant responsable d'assurer la résilience de son réseau, avec des moyens d'ampleurs plus limitées, qui pourront nécessiter de nouvelles formes de mutualisation.

Levier : Penser la résilience des réseaux

Le cadre de régulation actuel inclut la question de la résilience des réseaux, c'est à dire de la capacité des opérateurs à résister aux pannes qu'ils peuvent subir ou aux événements naturels. Les opérateurs sont soumis à des obligations de permanence, de qualité, de disponibilité, de sécurité et d'intégrité de leurs réseaux et services. Toute atteinte à la sécurité ou à l'intégrité des réseaux et des services doit être notifiée aux autorités compétentes. Une

réflexion pourrait être menée sur le caractère suffisant des obligations et mécanismes de surveillance actuels.

Les contributeurs sont invités à exprimer leurs remarques sur les objectifs et leviers décrits ci-dessus. Les contributeurs sont en particulier invités à exprimer dans leur réponse leur opinion sur les problématiques suivantes :

- Comment garantir la fiabilité des réseaux de communications électroniques ?
- Quel rôle doit jouer l'ARCEP sur ce sujet le cas échéant ?

2. La réponse

2.1. Importance de la fiabilité des réseaux

Les fortes intempéries d'octobre dernier dans la région de Cannes ont fortement perturbé internet, la téléphonie mobile et relancé par la même occasion le (vieux) débat sur la sécurité ou la fiabilité des réseaux de communications électroniques en France³. Avec près de 80% de la population ayant accès à internet⁴, de 26 millions d'abonnement internet à haut et

³ Le samedi 3 et 4 octobre 2015, de fortes intempéries ont touché le sud-est de la France, entraînant plus de 16 morts et de nombreux dégâts sur les infrastructures des réseaux de communications électroniques. Pour un aperçu de l'étendue de ces dégâts voir <http://pro.clubic.com/entreprises/orange-france-telecom/actualite-781880-degats-sud-point-situation-reseau-telephonique.html>.

Parmi les grands événements qui ont suscité de vives polémiques sur la fiabilité des réseaux, il peut être fait mention, de façon bien entendu non exhaustive, des tempêtes de 1999 qui ont secoué la France (environ 1. 12 milliards de francs de dégâts causés aux seuls réseaux de communications électroniques, 1 millions d'abonnés privés de téléphone fixe. Il a fallu attendre une semaine pour que les choses rentrent dans l'ordre. Par ailleurs, du 30 au 31 octobre 2004, France Télécom (aujourd'hui Orange) a connu un dysfonctionnement partiel de ses commutateurs conduisant à un échec des appels « arrivée ». Le 17 novembre de la même année, Bouygues Télécom a connu aussi une panne similaire affectant l'ensemble des abonnés (7 millions) sur les appels « arrivée » et « sortie ». Pour plus de détails, voir le *Rapport sur la résilience des réseaux de télécommunications du Conseil Nationale pour la Sécurité Civile*, juin 2007, 44 p., p. 8 ; *Rapport de la mission interministérielle chargé de l'évaluation des dispositifs de secours et d'intervention mis en œuvre à l'occasion des tempêtes* des 26 et 28 décembre 1999, juillet 2000 ; GIRAUD (J.-B.), « Orange, Free, Blackberry, Bouygues Télécom : histoires de pannes », *EcoQuick* du 07/07/2012. <http://www.economiematin.fr/news-orange-mobile-panne-reseau-blackberry-bouygues-telecom>.

⁴ Selon une étude menée par Internet World Stats sur l'utilisation de l'internet en Europe <http://www.internetworldstats.com/stats4.htm>. Une augmentation remarquable par rapport à 2012 où le pourcentage tournait autour des 75% http://www.insee.fr/fr/themes/document.asp?ref_id=ip1452. Voir aussi dans une perspective plus large et plus détaillée, l'enquête communautaire sur l'usage des TIC par les ménages et

très haut débit⁵, de 200 milliards de SMS et MMS envoyés ; et près de 238 milliards de minute de communications fixes et mobiles en 2014 selon l'ARCEP⁶, il est à peine besoin de dire que la France et les Français sont devenus dépendants des communications électroniques. Il va alors sans dire que toute défaillance (panne, attaque sur la disponibilité ou sur le fonctionnement des réseaux), qu'elle soit d'origine matérielle⁷, logicielle interne⁸ ou externe⁹, susceptible d'avoir un impact négatif sur la fiabilité – ou plus exactement sur la disponibilité –¹⁰ constitue de réelles sources de préoccupations. C'est qu'une défaillance sur un réseau, outre les conséquences dommageables qu'elle est à même d'avoir sur ce qu'on a coutume de nommer les « utilities » (l'eau, l'électricité et le transport), induit pour l'opérateur un manque à gagner en terme aussi bien économique (réparations des infrastructures, dédommagement des abonnés¹¹) que d'image¹². Mais ce n'est pas tout. Sur le plan juridique, la question de la

les particuliers de Eurostat en 2013, <http://www.observatoire-du-numerique.fr/usages-2/grand-public/equipement>.

⁵ Rapport d'activité de l'ARCEP 2014, p. 72, http://www.arcep.fr/uploads/tx_gspublication/rapport-activite-2014.pdf

⁶ *Ibid*, p. 73. http://www.arcep.fr/uploads/tx_gspublication/rapport-activite-2014.pdf.

⁷ Par exemple des coupures de câbles ou de fibres, des sites hors service lors des tempêtes de 1999 (Cf. note n°1).

⁸ Par exemple le dysfonctionnement partiel des commutateurs de France Telecom (Orange) conduisant à un échec des appels « arrivée » (*Rapport sur la résilience des réseaux de télécommunications, op. cit.*, p. 9).

⁹ Par exemple le ver *Slammer*, entraînant un déni de service, avait fortement perturbé internet en Janvier 2003.

¹⁰ C'est-à-dire la probabilité qu'un réseau de communications électroniques soit dans un état de bon fonctionnement à un instant *T*. La doctrine préfère plutôt parler, en ce qui concerne les communications électroniques, d'un problème de disponibilité que de fiabilité. Sur cette nuance, voir FICHE (G.), HEBUTERNE (G.), *Trafic et performances des réseaux de télécoms*, GET et Lavoisier, Collection Technique et Scientifique des Télécommunications (CTST), Paris, 2003, 583 p., p.222. Sur la question plus précise de la fiabilité voir en particulier le chapitre 6, pp. 221-265.

¹¹ Voir les problèmes de dédommagement (http://lexpansion.lexpress.fr/high-tech/quels-sont-vos-droits-en-cas-de-panne-de-telephone-ou-d-internet_1430337.html) lors de la « méga panne » du réseau d'Orange de 2012 (http://lexpansion.lexpress.fr/high-tech/les-raisons-de-la-mega-panne-chez-orange_1441852.html).

¹² En 2011, 50 millions d'utilisateurs BlackBerry, un peu partout dans le monde, se sont retrouvés privés de messagerie pendant 3 jours, du 10 au 13 octobre 2011. Cela lui a

fiabilité des réseaux des communications électroniques suscite des réflexions très sérieuses sur le respect de la liberté d'expression et du secret des correspondances et dans une certaine mesure, sur le respect de la vie privée et la protection des données à caractère personnel¹³. Et si ces questions semblent, *prima facie*, ressortir de la CNIL¹⁴, il serait cependant réducteur de limiter celles-ci à celle-là. En réalité, la fiabilité des réseaux implique forcément la question de leur résilience¹⁵ et ramène donc en boucle au rôle du gendarme des communications électroniques : l'ARCEP.

2.2. Organisation de l'obligation de notification des défaillances de réseaux

Une intervention a priori de l'ARCEP dans le contrôle de la fiabilité des réseaux est envisageable à travers des procédures d'inspection régulière. Si l'ARCEP conduit d'ores et déjà des campagnes de vérification de la fiabilité des cartes de couverture, elle peut mettre des audits préventifs de sécurité des réseaux. Néanmoins, le déploiement de moyens humains et matériels nécessaires à ces inspections apparaît fort coûteux et ne garantit pas l'absence totale de défaillance. Une intervention a posteriori serait plus adaptée. Elle pourrait se traduire par l'élaboration de deux obligations à la charge des fournisseurs de services de communications électroniques, notamment les opérateurs, à l'instar des obligations qui pèsent sur le responsable des traitements de données personnelles dans la loi n° 78-17 du 6 janvier 1978

fait perdre sa place dans le club des constructeurs leader de smartphone. Cf GIRAUD (J.-B.), « Orange, Free, Blackberry, Bouygues Télécom : histoires de pannes », *op. cit.*,

¹³ Concernant les questions juridiques que peut soulever cette question de fiabilité des réseaux, voir la chronique suite aux pannes téléphoniques en France fin 2004 de GRIBOFF (N.), « Pannes de réseaux téléphoniques : responsabilité des opérateurs et droits des consommateurs », *Espace Télécom*. <http://junon.u-3mrs.fr/u3ired01/Main%20docu/telecom-chroniq-nico.htm>.

¹⁴ L'article 34 bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés fait en effet référence aux fournisseurs de services de communications électroniques.

¹⁵ Sur cette question voir le *Rapport sur la résilience des réseaux de télécommunications du Conseil Nationale pour la Sécurité Civile*, juin 2007, 44 p.

relative à l'informatique, aux fichiers et aux libertés : une obligation de sécurité des réseaux, déjà introduite dans le Code des postes et des communications électroniques¹⁶, et une obligation de notification en cas de défaillance des réseaux. Il incomberait à l'ARCEP de veiller au respect de ces obligations tandis que la CNIL resterait compétente en matière de violation des données personnelles.

On entend par la défaillance du réseau toute atteinte au réseau affaiblissant voire neutralisant ses performances qu'elle soit d'origine criminelle ou accidentelle.

Par l'origine criminelle de la défaillance du réseau, on entend toute infraction pénale commise sur les réseaux de communications électroniques de tout type.

Par l'origine accidentelle de la défaillance du réseau, on entend tout événement fortuit ou survenu par négligence sur le réseau de communications électroniques.

En cas de survenance d'une défaillance du réseau de communications électroniques, tout opérateur tel que défini à l'article L.32 du Code des postes et des communications électroniques, devra avertir sans délai l'ARCEP.

Cette notification n'est toutefois pas nécessaire si la défaillance est d'ampleur minime. En effet, compte tenu de la technicité du domaine dont il est question, il serait opportun de mettre en place une doctrine *de minimis* en tenant compte de la zone géographique touchée, de l'ampleur et de la durée de la défaillance. Cela permettrait ainsi de ne pas noyer la notification de défaillances importantes dans la masse des défaillances qui n'ont pas de véritable effet, et de ne pas décrédibiliser les opérateurs pour des défaillances d'importance mineure.

A défaut de notification, l'ARCEP pourra le cas échéant prendre les mesures nécessaires dont des sanctions administratives à déterminer. Par analogie avec l'article 226-

16 Art. L.33-1 alinéa 5 du Code des postes et des communications électroniques

17-1 du code pénal¹⁷, le défaut de notification d'une défaillance réseaux de la part de l'opérateur pourra également être passible d'une sanction pénale.

2.3. Publication des défaillances de réseaux

Il est possible de notifier une défaillance des réseaux directement à l'utilisateur. Cette notification peut être effectuée soit par l'ARCEP, soit par l'opérateur lui-même. Cependant, les utilisateurs potentiels peuvent également avoir besoin de connaître l'existence de défaillances des réseaux pour faire un choix parmi les différentes offres des opérateurs. Or si la notification ne concerne que les utilisateurs actuels, les utilisateurs potentiels se verraient privés d'informations essentielles. Il est donc possible d'envisager une publication de ces défaillances sur le site web de l'ARCEP. Cette publication devrait mentionner l'origine de la défaillance et l'opérateur concerné. Il faudrait s'interroger sur l'ampleur de la divulgation, car donner trop de détails sur les modalités de la défaillance, si elle découle d'une cyberattaque, pourrait avoir un effet contre-productif en donnant des idées à certains individus mal-intentionnés. S'agissant des opérateurs, l'anonymisation peut être envisagée dans le cas d'une attaque qui serait propre à un protocole et qui toucherait plusieurs opérateurs. En revanche, dans les autres cas, elle ne semble pas être la bienvenue. En effet, on peut se demander si une publication anonymisée ne serait pas vidée de son objet : la valeur informative en serait fortement diminuée car les utilisateurs ne sauraient alors pas quel réseau est affecté. En outre, cette publication perdrait également sa fonction d'incitation des opérateurs à la prévention des défaillances puisqu'ils ne seraient pas nommément désignés et qu'il n'y aurait dès lors pas de risque pour leur image.

17 Art. 226-17-1 Code pénal : Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

La publication, qui relèverait de la compétence de l'ARCEP, pourrait faire l'objet d'un contrôle avant sa mise en ligne sur le site Internet de celle-ci par l'ANSSI, dans le cas d'une défaillance due à une cyberattaque, afin d'éviter que des informations qui pourraient à l'avenir mettre en péril des réseaux soient divulguées. L'ANSSI pourrait également disposer d'un pouvoir de veto quant à la divulgation de certaines informations stratégiques pour les intérêts du pays.

En conclusion et en synthèse

Dans la mesure où les réseaux de communications électroniques sont essentiels pour notre société, leur fiabilité doit être garantie. Il peut être judicieux de confier un rôle à l'ARCEP dans ce domaine, en la chargeant de veiller au respect d'une obligation de sécurité des réseaux et d'une obligation de notification des défaillances, criminelles comme accidentelles. Le constat pourrait être suivi de sanctions (pénales ou administratives) ainsi que d'une publication sur le site de l'ARCEP.