Confiance Numérique

Assurer la prochaine vague de croissance numérique

LIBERTYGLOBAL
POLICY SERIES

booz&co.

Confiance Numérique

Assurer la prochaine vague de croissance numérique

Traduit de l'anglais

LA CONFIANCE NUMÉRIQUE – QUELQUES NOTIONS CLÉS

• Dans le domaine de l'économie numérique en Europe, une croissance de 18 % par an est attendue d'ici à 2012 pour atteindre un volume de 436 milliards d'€ par rapport à 236 milliards d'€ en 2008.

• Jusqu'à présent, la croissance de l'économie numérique était en majeure partie due à une extension des infrastructures et au développement technologique tels que le passage à la télévision numérique et les technologies haut débit de nouvelles générations.

• À l'avenir, on observera une modification très importante des valeurs au-delà de l'accès – bien qu'encore très profitable et en croissance d'un chiffre – vers le commerce électronique, les offres de contenus en ligne et numériques et la publicité en ligne.

• L'augmentation de l'usage et des dépenses par utilisateur sera le moteur de la croissance dans les 5 prochaines années : les marchés du contenu et de la publicité présenteront des taux de croissance à deux chiffres. Le e-commerce demeurera le marché le plus grand en valeur absolue.

• Ces facteurs de croissance devront prévaloir face à des forces perturbatrices majeures au sein de la Société Européenne de l'Information, tels que les services du Web 2.0 qui convergent sur différentes platesformes (Internet, la télévision numérique ou le mobile) et une nouvelle génération de consommateurs « nés à l'ère du numérique », hyperconnectés et résolument participatifs mais également très affirmés à travers d'une expression au sein de la presse et d'actions politiques.

• Le succès de l'économie numérique a cependant généré de nombreuses préoccupations pour les consommateurs et les entreprises en ce qui concerne la sécurité et l'intégrité de l'environnement numérique.

• Pour cette raison, l'augmentation de la Confiance Numérique devient un facteur clé de la croissance – ou un frein à celle-ci – au sein de l'économie numérique, de même qu'elle permet de mesurer à quel point les consommateurs et les fournisseurs se fient aux services numériques et aux services en ligne. Un volume de marché de 124 milliards d'€ (2012) pourrait être en danger, approximativement 1 % du PIB pour l'UE des 27, avec une valeur de marché liée aux contenus et à la publicité étant extrêmement exposée. Le potentiel de hausse économique en cas de succès dans l'augmentation de la confiance s'élève à une croissance supplémentaire de 11 % (ou 46 milliards d'€) en plus des 436 milliards d'€ du cas de base. Le désavantage en cas d'échec dans la tentative d'augmenter la Confiance Numérique est cependant plus grand ; 18 % (ou 78 milliards d'€) pourraient être perdus ou différés de manière significative.

• Tous les acteurs de l'industrie sont d'accord quant à l'importance de constituer des références à la Confiance Numérique et ont en conséquence déployé une large palette d'activités – actuellement, il existe cependant une lacune claire en matière de cohérence et de mise au point commune, étant donné que la majorité des actions sont effectuées seulement lorsque les circonstances l'exigent, déclenchées par de graves incidents au sein de la confiance ou par des disfonctionnements en matière de sécurité et sous la pression politique.

• La législation ne peut pas faire face à elle seule à la rapidité et à l'envergure des défis sur ce marché. De ce fait, les entreprises qui réussissent ne se contentent pas de se conformer à la législation, elles essaient en outre d'avoir une longueur d'avance en adoptant des politiques et des pratiques proactives pour gérer la Confiance Numérique.

• La Confiance Numérique est bâtie sur quatre piliers qui, tous ensemble, abordent les domaines les plus vitaux des préoccupations des consommateurs et de l'industrie :

1. Intégrité du réseau et qualité du service (QdS) – visant en particulier à fournir des platesformes technologiques sécurisées et flexibles pour l'économie numérique et à procurer une expérience client optimale.

2. Protection de la vie privée et des données – concernant les problèmes de la sécurité des individus et le respect de leurs données numériques.
3. Protection des mineurs – visant à défendre le bien-être des mineurs au sein de l'univers internet.
4. Prévention contre la piraterie et le vol – visant à offrir à toutes les parties prenantes un environnement sécurisé de transactions numériques.

- En tant que parties en relation avec le client, les opérateurs de réseaux doivent relever le défi de mettre en place des politiques et des pratiques aptes à obtenir l'acceptation générale des utilisateurs, ceci allant au-delà de la simple observation des prescriptions légales ou de la défense des intérêts de certaines parties prenantes en particulier.

- Par conséquent, les politiques et pratiques ne devraient pas être établies en fonction de problèmes isolés (par ex. la piraterie) mais devraient au contraire refléter une vue holistique sur tous les domaines de la confiance numérique, étant donné que les implications de ces politiques convergent dans la pratique et qu'elles se sont montrées susceptibles de produire des réactions contradictoires de la part des parties prenantes.

- Les leçons clés ressortant d'études de cas réalisées partout dans le monde montrent qu'une vision « can-do » est réaliste : en ce qui concerne l'amélioration de la confiance numérique, les opérateurs de réseaux pourraient aller au-delà de leur rôle traditionnel de « simple conduit » et du rôle d'éducateur/enseignant, tout en observant les directives pour des pratiques acceptables pour le consommateur et en protégeant les havres légaux de sécurité.

- Sur la base des cas analysés, les meilleures pratiques du point de vue de l'acceptation par le consommateur ont la forme suivante :

  - Les consommateurs acceptent les pratiques qui sont transparentes et qui s'avèrent discrètes : les opérateurs de réseaux et de platesformes et les fournisseurs de contenus, conjointement avec les organes de régulation, se doivent de faire avancer une telle communication.

  - Les consommateurs sont préoccupés par la question de savoir comment les opérateurs de réseaux gèrent et protègent les données numériques des consommateurs : des déclarations claires et une structure de régulation consistante et fiable semblent être ici une priorité absolue.

  - Les consommateurs exigent un contrôle des risques auxquels ils sont exposés : ceci rend nécessaire un accès aux outils adéquats, des mécanismes d'opt-in/opt-out et une certaine éducation du consommateur.

  - Les consommateurs acceptent les mesures qui garantissent un service de qualité : si ceci requiert une gestion active des opérations, ils sont alors ouverts à une telle démarche, à condition que les conditions du service soient communiquées ouvertement.

- Afin de garantir des niveaux d'intervention proportionnés et afin d'obtenir une acceptation générale de l'utilisateur, lorsqu'ils adoptent plus de politiques de pratiques proactives, les opérateurs de réseaux devraient utiliser une approche progressive en appliquant le paradigme suivant : éduquer d'abord, responsabiliser ensuite, puis imposer de manière sélective si nécessaire.

- Les politiques et pratiques en matière de confiance numérique doivent être intégrées au sein des organisations respectives en établissant des protocoles internes et des structures de gouvernance afin de guider le développement des produits et services ; le choix et le déploiement de technologies basées sur les réseaux et les solutions de sécurité, et la communication avec les clients et les autres parties prenantes (leaders du secteur, propriétaires de contenus, régulateurs).

I. RÉSUMÉ GÉNÉRAL

LA PROCHAINE VAGUE DE CROISSANCE DANS LE MONDE DU NUMÉRIQUE : C'EST L'USAGE QUI MÈNE LA CROISSANCE ET NON PAS LE NOMBRE D'UTILISATEURS

L'économie numérique européenne a une perspective réaliste de croissance stimulée par les services de type Web 2.0 qui sont devenus la tendance dominante en utilisant la fonctionnalité, l'omniprésence et les nouvelles capacités des réseaux haut débit. La transition vers des réseaux d'accès nouvelle génération, la prolifération de technologies de réseaux hautement sophistiquées et la nouvelle génération de consommateurs « nés à l'ère du numérique » et dotés d'une très grande assurance constituent des forces potentiellement perturbatrices pour l'écosystème de l'économie numérique. Ce nouveau paradigme est un défi considérable aussi bien pour l'industrie au sens large que pour les responsables des politiques appliquées et les régulateurs.

Les enjeux sont considérables : nous prévoyons que le marché européen des services numériques atteigne 436 milliards d'€ en 2012, avec un taux de croissance composé annuel de 18 % (2007-2012).

Jusqu'à présent, la croissance de la consommation Internet a été largement soutenue par l'extension des nouvelles technologies (accès haut débit et télévision numérique). Les producteurs de technologie actuels ont amené les niveaux de pénétration des accès à Internet à la quasi saturation sur de nombreux marchés. Ainsi, la prochaine vague de croissance numérique sera essentiellement portée par une augmentation des recettes générée par la stimulation des dépenses des utilisateurs plutôt que par une augmentation du nombre d'utilisateurs. Il est prévu que cette croissance s'accomplisse grâce à des produits et des services plus innovants, complétés par des nouveaux modèles économiques à même de générer des sources de revenus supplémentaires. Les principaux secteurs de croissance économique identifiés sont, dans l'ordre de leurs taux de croissance respectifs : la publicité, les contenus, le e-commerce et l'accès internet.

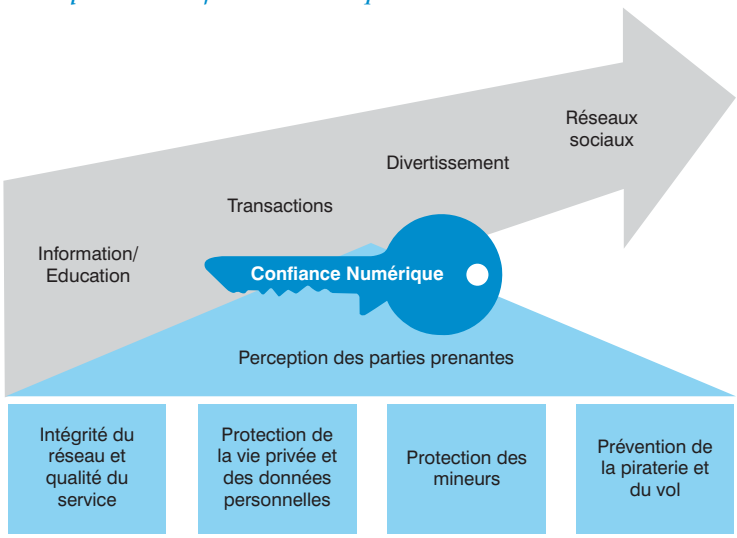
Conjointement au succès de l'économie numérique sont apparues de nombreuses préoccupations pour les consommateurs et les entreprises, notamment en relation avec la sécurité et l'intégrité de l'environnement numérique. Le degré de confiance accordé par les consommateurs aux fournisseurs d'accès et de platesformes en termes de maintien du service et de fourniture d'environnements de réseaux et de services sécurisés, aussi bien que celui accordé aux gouvernements et aux autorités de régulation quant à l'aptitude à faire respecter les standards de protection des consommateurs, devient un paramètre majeur affectant le potentiel de croissance de l'économie numérique.

Il est un besoin urgent de développer une vue commune des priorités dans le domaine de l'amélioration de la confiance et de la sécurité, des rôles et responsabilités pouvant et devant être assumés par chaque acteur, de même qu'une entente concernant les outils et mesures appropriés pouvant et devant être appliqués. L'objectif de ce rapport est de fournir un ensemble de faits en vue du débat et d'introduire des structures, un langage commun et des idées destinés à faciliter une vision commune et des politiques et actions jointes – ou coordonnées – là où celles-ci sont nécessaires.

CONFIANCE NUMÉRIQUE : ASSURER LA CROISSANCE FUTURE DE L'ÉCONOMIE NUMÉRIQUE

Sur cette toile de fond, la promotion et l'amélioration de la confiance et de la sécurité deviennent un facteur clé de la croissance future de l'économie numérique. Ceci est particulièrement important du fait que les consommateurs « nés à l'ère du numérique » s'affirment de plus en plus en réduisant leur propre consommation,

Concept de la Confiance Numérique



en alimentant la presse ou même en appuyant certaines actions politiques – souvent en tirant profit des technologies Web 2.0. Sur la base d'entretiens réalisés auprès de 50 experts européens et américains, et d'une étude de marché fondée sur l'analyse de données et la revue des meilleures pratiques et des perspectives de l'industrie, nous avons identifié quatre piliers interdépendants répondant, aujourd'hui et demain, aux principales problématiques des consommateurs et de l'industrie en matière d'économie numérique :

- La **garantie de l'intégrité du réseau et de la qualité du service** pour les consommateurs et les entreprises, dans la mesure où ceci est lié à la protection des platesformes technologiques contre toutes attaques criminelles portant atteinte à la sécurité, en vue de garantir une connectivité Internet optimale malgré les surcharges de trafic ou les attaques criminelles externes, en vue de sécuriser l'environnement informatique pour les consommateurs individuels comme pour les entreprises contre toutes perturbations dues à des virus ou autres logiciels malveillants.

- La **protection de la vie privée et des données personnelles,** c.-à-d. protéger les données électroniques privées des consommateurs (identité, mots de passe, profils d'usage et de consommation, etc.) contre l'accès illicite, la publication ou l'exploitation commerciale sans consentement, et prévenir le vol d'identité et la fraude.

- La **protection des mineurs,** c.-à-d. protéger les enfants de toute exposition à des contenus indésirables, empêcher le harcèlement et tout autre comportement hostile, empêcher le grooming (c.-à-d. l'utilisation de sites de rencontres en ligne par des adultes cherchant à séduire des mineurs) ou tout autre forme de sollicitation d'enfants par des adultes et lutter contre les contenus de pornographie enfantine.

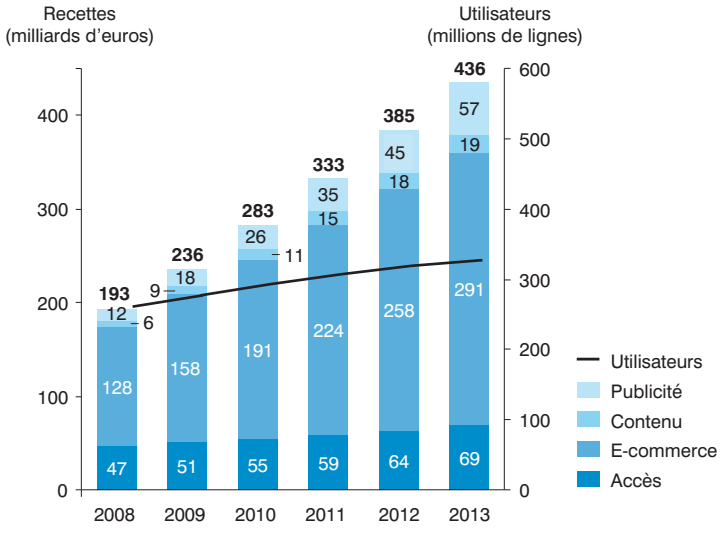
- La **prévention de la piraterie et du vol,** c.à-d. enrayer le vol de contenus protégés par des droits d'auteur et sécuriser les transactions e-commerce pour toutes les parties engagées.

L'industrie a besoin d'agir de manière proactive sur la base d'une vision holistique de toutes ces questions. Cette approche se retrouve dans le concept de « Confiance Numérique ». Promouvoir la Confiance Numérique dépasse largement la simple observation des prescriptions légales – cela devient presque un préalable commercial et l'équivalent d'un permis d'agir. Comme certaines études de cas le montreront, l'observation des prescriptions légales ne permet pas à elle seule d'obtenir l'acceptation du consommateur. Les politiques des opérateurs et les pratiques commerciales se doivent d'aborder tous les questions légales, économiques et publiques associés à ces domaines de manière conjointe et cohérente, afin de permettre la prochaine phase de croissance de l'économie numérique.

ANALYSE DES RISQUES ET BÉNÉFICES : LA CONFIANCE NUMÉRIQUE EST RENTABLE

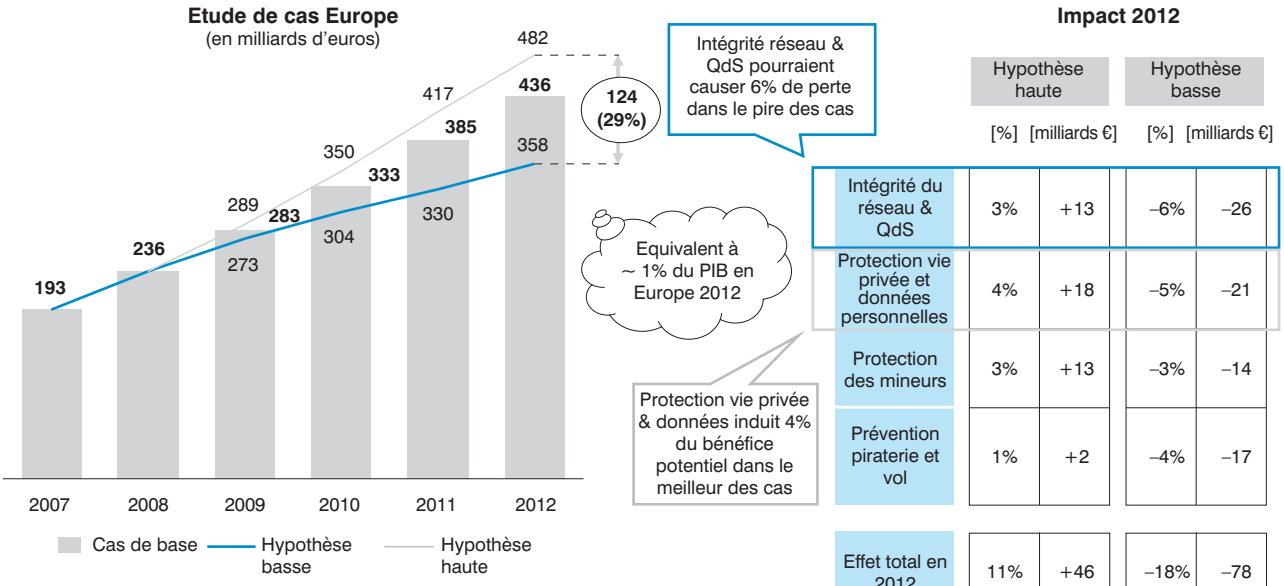
Conformément à la recherche et aux analyses de Booz & Company, l'enjeu est un marché de 436 milliards d'€ en Europe jusqu'en 2012, avec un taux de croissance composé annuel de 18 %, (marchés d'accès Internet, e-commerce, contenus et publicité en ligne). La différence de revenus entre un scénario optimiste de « réussir la Confiance Numérique » et un scénario pessimiste de « la voir échouer » s'élève à 124 milliards d'€, soit presque 30 % du marché total en jeu – approximativement 1 % du PIB total de l'UE-27+2 en 2012 ! L'effet d'un échec dans l'établissement de la Confiance Numérique est, avec 78 milliards d'€, nettement plus grand que l'impact du scénario le plus optimiste, chiffré à 46 milliards d'€ – sous l'influence primaire des effets des piliers « Intégrité du réseau et qualité du service » et « Protection de la vie privée et des données », qui ont un impact sur tous les types de revenus de l'économie numérique et sur le niveau d'utilisation et le nombre d'utilisateurs dans les principales catégories de recettes.

Vie numérique—total des revenus en Europe



Note : Europe, comprenant l'UE à 27, la Norvège et la Suisse
Source : Forrester e-Commerce Forecast, rapports d'Apple, rapports de Google, EU TV et modèle prévisionnel haut débit, analyse Booz & Company

Impact de la Confiance Numérique



Impact 2012

	Hypothèse haute		Hypothèse basse	
	[%]	[milliards €]	[%]	[milliards €]
Intégrité du réseau & QdS	3%	+13	–6%	–26
Protection vie privée et données personnelles	4%	+18	–5%	–21
Protection des mineurs	3%	+13	–3%	–14
Prévention piraterie et vol	1%	+2	–4%	–17
Effet total en 2012	11%	+46	–18%	–78

Note : PIB Europe 2012 estimé à 12,5–13,5 tn EUR (Europe : UE-27 + Norvège + Suisse
Source : Ovum, analyse Booz & Company

La « Protection de la vie privée et des données » est financièrement importante, spécialement mais non exclusivement en raison de ses implications dans les modèles économiques de publicité innovante (ciblée). Les consommateurs pourraient perdre l'envie de faire des achats sur Internet, d'acheter des contenus en ligne ou de souscrire à des services numériques innovants s'il existe un manque de confiance concernant la façon dont leurs données personnelles sont traitées et sécurisées. L' « Intégrité du réseau et la qualité du service » seront nécessaires pour soutenir la continuité de la croissance des offres de contenus et vidéos. Bien gérés, les réseaux peuvent de fournir du haut débit et une qualité de service offrant à tous les utilisateurs un accès au monde d'Internet. Le domaine de la « Prévention de la piraterie et du vol » est pertinent aussi bien pour les propriétaires de contenus que pour le e-commerce. En dehors des implications évidentes, en termes de revenus pour l'industrie des contenus, de la protection de la valeur existante de leurs portefeuilles de droits et de l'introduction de modèles économiques innovants de contenus numériques, il existe un risque significatif sur les transactions de e-commerce portant sur les consommateurs pouvant se tourner vers des réseaux de ventes physiques, ce qui reste possible pour un grand nombre de nouveaux modèles économiques (par ex. enchères en ligne).

Les catégories de revenus les plus sensibles par rapport à la Confiance Numérique sont les marchés des contenus et de la publicité. Les deux marchés en sont au stade naissant et leur développement est hautement dépendant de la Confiance Numérique : la publicité pourrait être sévèrement entravée par des réactions défavorables de consommateurs si elle n'est pas implé-mentée selon des méthodes qui obtiennent globalement l'acceptation des utilisateurs, ou en cas de législation trop restrictive. Par exemple, le fait de protéger la vie privée des consommateurs de manière très restrictive pourrait avoir un impact sur les nouveaux modèles économiques basés sur la publicité ciblée et personnalisée – un facteur contribuant essentiellement au marché de la publicité en ligne chiffré à 57 milliards d'€ en Europe en 2012. De plus, la publicité jouera un rôle central dans la monétisation de tous les services Web 2.0 émergeants et présentant une croissance rapide, tels que les sites de réseaux sociaux ou les offres de contenus inno-vantes. Les fournisseurs de contenus craignent le fait qu'une piraterie excessive pourrait fondamentalement mettre en danger leurs modèles économiques numériques. Le e-commerce est relativement moins exposé, mais il présente l'impact absolu le plus élevé en raison de son important volume d'affaires, contribuant à la baisse à hauteur de 52 milliards d'€, et à hauteur de la moitié de cette somme à la hausse potentielle liée à la Confiance Numérique.

Pour parler en termes purement économiques en laissant de côté pour le moment les aspects sociétaux plus larges, l'analyse des risques et des bénéfices montre que l'industrie du numérique a une motivation économique considérable devant l'inciter à aborder de manière cohérente toutes les

questions relatives au thème de la Confiance Numérique, au moins pour éviter le scénario le plus pessimiste en termes de revenus et, dans l'idéal, pour atteindre le potentiel de recettes du scénario le plus optimiste.

Tous les acteurs de l'industrie s'accordent sur l'importance de constituer des références à la Confiance Numérique et ont en conséquence déployé une large palette d'activités – actuellement, il existe cependant une lacune claire en matière de cohérence et de mise au point commune, étant donné que la majorité des actions sont effectuées seulement lorsque les circonstances l'exigent, déclenchées par de graves incidents au sein de la confiance ou par des atteintes à la sécurité et sous la pression politique.

La distinction essentielle entre les scénarios les plus optimistes et les plus pessimistes est le degré d'alignement entre les acteurs de l'industrie dans leur approche de la Confiance Numérique. L'alignement ne signifie pas nécessairement que les acteurs doivent agir en tout point de manière identique ; il s'agit plutôt du degré d'accord au sein de l'industrie en vue de suivre une même direction. Cela se rapporte à la mesure dans laquelle il existe une entente commune concernant une telle direction à suivre et les priorités globales de même que les responsabilités en résultant pour chacune des parties prenantes.

Les fournisseurs de réseaux doivent continuer à jouer un rôle important étant donné que leur cœur d'activité est un élément clé les facteurs de croissance économique identifiés. Le degré d'intégrité des réseaux a un impact économique majeur même si leur cœur de métier, l'accès, semble moins exposé aux bénéfices et aux risques liés à la réussite ou à l'échec de la Confiance Numérique.

CADRE D'ACTION

Les quatre piliers de la Confiance Numérique doivent être abordés en étant considérés comme des points urgents. Ils sont extrêmement interdépendants et tous les domaines contribuent à une conscience globale du monde numérique comme étant un lieu sûr – ou ne l'étant pas.

En raison de la complexité des problèmes impliqués et de l'interdépendance de nombreux acteurs tout au long de la chaîne de création de valeur, il devient évident que chacun doit jouer son rôle au sein de l'économie numérique. Bien que les opérateurs de réseaux contribuent, dans de nombreux domaines, à fournir une solution, il est cependant clair qu'ils ne peuvent qu'apporter leur propre pièce au puzzle global.

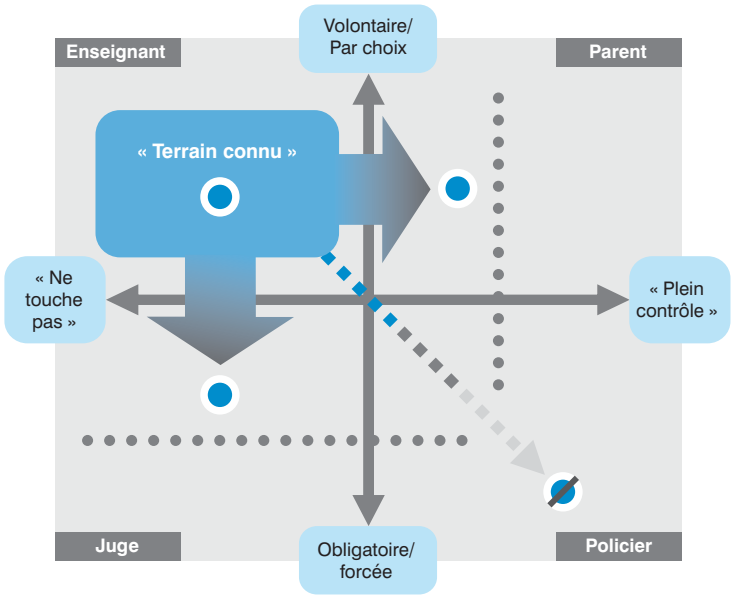
En vue de schématiser les divers rôles pouvant être joués par les opérateurs de réseaux dans les domaines identifiés de la question, un « Cadre de positionnement de la Confiance Numérique » a été développé. Ce cadre représente la manière dont sont prises les mesures (par ex. passivement selon le principe de la « non-intervention » ou activement selon une méthode de « plein contrôle ») et différencie les principes sous-jacents. Les différents rôles en résultant peuvent être clairement reliés à des rôles sociétaux génériques. Par exemple :

- L'Enseignant éduque autant que possible les utilisateurs au sujet des opportunités et des menaces, mais ne prendra normalement aucune mesure corrective active (par ex. « Web Wise Kids » produisant du matériel éducatif pour les enfants sur Internet).

- Le Parent éduque les utilisateurs au sujet des menaces et des mesures de manière similaire à l'Enseignant, mais prendra des mesures de manière proactive si cela est jugé nécessaire pour protéger les utilisateurs (par ex. YouTube filtrant les contenus protégés par copyright).

- Le Juge se base sur une mise en application autoimposée de règles au cas par cas et sur des directives plutôt que sur l'éducation, mais les règles sont basées sur des accords mutuels (par ex. UPC NL restreignant de manière proac-tive l'accès aux domaines ayant des contenus de pornographie enfantine).

Positions des opérateurs de réseaux



• Le Policier est naturellement enclin à une mise en application forte basée sur le mandat légal, il prend toutes les mesures nécessaires et agit en se basant sur des règles strictes, par ex. en bloquant toutes les activités illégales (par ex. l'implémentation d'une règle de « riposte graduée et vous êtes dehors » en cas de violation du copyright).

Tout en définissant leurs positions dans ce champ, les opérateurs de réseaux doivent cependant être très prudents lorsqu'il s'agit pour eux d'assumer des rôles en dehors de leur activité commerciale et de leurs responsabilités primaires. Tout geste susceptible d'ébranler leur havre sûr de « simple tuyau » et de les exposer à des responsabilités incontrôlables annihilera, en fin de compte, leur contribution à l'amélioration de la confiance numérique – bien que les attentes au sein du public eussent été augmentées.

Sur la base de notre analyse des succès et des échecs dans le domaine de la Confiance Numérique, il semble y avoir dans ces dimensions un « terrain connu » traditionnel – un environnement naturel – pour les opérateurs de réseaux : la position dénommée celle de l'« Enseignant », qui met autant que possible l'accent sur l'éducation des utilisateurs au sujet des opportunités et des menaces, mais qui ne prendra normalement aucune mesure corrective proactive. Ce terrain connu serait ensuite uniquement quitté pour garantir le respect des prescriptions légales. Mais notre analyse montre clairement que ceci ne sera pas suffisant à l'avenir.

Fréquemment, la législation ne peut pas faire face à elle seule à la rapidité et à l'envergure des changements liés à la Confiance Numérique. En tant que parties en relation avec le client, les opérateurs de réseaux doivent assumer le défi de mettre en place des politiques et des pratiques aptes à obtenir l'acceptation générale des utilisateurs, ceci allant au-delà de la simple observation des prescriptions légales ou de la défense des intérêts de certaines parties prenantes en particulier.

De ce fait, les entreprises qui réussissent ne se contentent pas de se conformer à la législation, elles essaient en outre d'avoir une longueur d'avance en adoptant certains principes clés pour gérer la Confiance Numérique :

• Elles agissent en confiance en mettant en place des procédures et des protocoles.

• Elles sont aussi ouvertes et transparentes que possible dans leur communication avec les consommateurs.

• Elles accomplissent un effort supplémentaire pour éduquer les consommateurs et leur per-mettre de protéger leurs intérêts au sein de l'univers numérique.

Afin de garantir des niveaux d'intervention proportionnés et afin d'obtenir une acceptation générale de l'utilisateur, lorsqu'ils adoptent plus de politiques de pratiques proactives, les opérateurs de réseaux devraient également utiliser une approche progressive en appliquant le paradigme suivant : éduquer d'abord, responsabiliser ensuite, puis imposer de manière sélective si nécessaire.

Sur la base des cas analysés, les meilleures pratiques du point de vue de l'acceptation par le consommateur ont la forme suivante :

• Les consommateurs acceptent les pratiques qui sont transparentes et qui s'avèrent discrètes : les opérateurs de réseaux, fournisseurs de services, éditeurs de contenus et de platesformes, conjointement avec les organes de régulation, se doivent de faire avancer une telle communication.

• Les consommateurs sont préoccupés par la question de savoir comment les opérateurs de réseaux et FAI gèrent et maintiennent en ordre les données numériques des consommateurs : des déclarations claires et une structure de régulation consistante et fiable semblent être ici une priorité absolue.

• Les consommateurs exigent un contrôle des risques auxquels ils sont exposés : ceci rend nécessaire un accès aux outils adéquats, des mécanismes opt-in/opt-out et une certaine éducation du consommateur.

• Les consommateurs acceptent les mesures qui garantissent un service de qualité : si ceci requiert une gestion active des opérations, ils sont alors ouverts à une telle démarche, à condition que les conditions du service soient équitables, transparentes et communiquées ouvertement.

Ces principes sont applicables à toutes les parties prenantes.

Lors d'une étape suivante, les politiques et pratiques de la Confiance Numérique doivent être intégrées au sein des organisations respectives. Après exploration des implications pour les opérateurs de réseaux, il apparaît essentiel d'aligner les activités afin d'accéder au niveau supérieur dans la Confiance Numérique. Les fournisseurs doivent agir à cinq niveaux :

1. POLITIQUES ET PROCÉDURES

Les opérateurs de réseaux et les FAI doivent affirmer leur positionnement dans la Confiance Numérique, définissant leur stratégie et leur position par rapport à chaque pilier de la confiance. Ceci doit être le fondement de toutes les politiques ayant trait à la Confiance Numérique. L'affirmation de positionnement doit être suffisamment précise pour fournir une direction tangible dans les questions sous-jacentes en relation avec ces problèmes, c.-à-d. comment une entreprise équilibre le compromis entre des contenus inappropriés et la liberté d'expression.

Lors d'une étape suivante, ces politiques doivent être intégrées au sein des processus centraux de l'entreprise. Dans la majorité des cas, ceci aura un impact direct sur la manière dont les opérateurs de réseaux appréhendent le développement des produits, par ex. en s'assurant que toutes les nouveautés en matière de produits et services répondent aux standards propres à l'entreprise.

En outre, les opérateurs de réseaux doivent s'assurer de l'actualité permanente des politiques et procédures de Confiance Numérique, en effectuant des remaniements réguliers des procédures et politiques légales, publiques et techniques existantes.

Enfin, dernier point mais non le moindre, les cas analysés dans ce rapport apportent un enseignement particulièrement important : la confiance est synonyme de foi, et la meilleure base pour cette foi est une communication ouverte ; la transparence est vraiment payante. En conséquence, les entreprises devraient se montrer ouvertes au sujet des politiques qu'elles appliquent et des logiques sur lesquelles elles se fondent – y compris les logiques économiques. L'expérience montre que l'acceptation par le consommateur est généralement élevée lorsque les règles et les logiques sous-jacentes sont ouvertement communiquées. Ceci permet en outre d'engager avec le consommateur un dialogue qui peut être très utile pour améliorer les solutions.

2. GOUVERNANCE

Les questions de Confiance Numérique sont complexes, très sensibles et interfonctionnelles par nature. Très fréquemment, il est nécessaire de définir exhaustivement les positions fondamentales de l'entreprise – par ex. comment traitons-nous les contenus de pornographie enfantine ? Négliger ceci implique des risques élevés au niveau financier comme au niveau de la réputation. De ce fait, il est extrêmement important que la Direction y accorde une attention suffisante. La Confiance Numérique doit être clairement intégrée à la structure organisationnelle, par exemple par le biais d'un Conseil de la Confiance Numérique doté d'une surveillance senior incluant une autorité de supervision et d'implémentation de toutes les activités en rapport.

3. TECHNOLOGIE

Les technologies permettant la Confiance Numérique sont largement mises en place, et l'attention principale doit être accordée aux décisions de positionnement individuel, de définition de politiques appropriées et d'établissement des structures de gouvernance encadrant le tout. Toutefois, la majorité des opérateurs de réseaux auront besoin de faire certains investissements sur le plan technologique afin de préparer le futur. Ceux-ci visent à assurer le maintien de la qualité du service malgré une augmentation du trafic multimédia. Les opérateurs de réseaux devront prendre des décisions d'investissement en gérant le compromis nécessaire entre une augmentation des capacités de transport et la gestion active du trafic, notamment par le biais de prix échelonnés ou de mesures techniques. Les opérateurs de réseaux et les FAI doivent coopérer avec les fournisseurs de contenus afin d'optimiser leurs réseaux pour la fourniture de contenus multimédias grâce à des technologies telles que les caches pair-à-pair (par ex. méthodes développées par l'initiative P4P) ou des réseaux de fourniture de contenus. Ils doivent s'assurer que les régulateurs comprennent bien qu'ils abordent la question de manière appropriée.

Un autre domaine de risque majeur sur le plan technologique s'avère être actuellement la question de l'équipement des utilisateurs finaux. Généralement, cet équipement n'est pas suffisamment protégé contre les menaces telles que les virus, les botnets et autres formes de logiciels malveillants. Il existe déjà des logiciels apportant une solution ; cependant, les fournisseurs de réseaux devraient encourager plus activement les clients à utiliser ceux-ci.

Les fournisseurs de services doivent par ailleurs déployer plus d'outils et de solutions permettant aux consommateurs de contrôler et de gérer leur propre degré d'exposition, par ex. par le biais de fonctions opt-in/opt-out. Ceci rendra nécessaire un changement au niveau des activités : il n'est pas suffisant d'offrir des solutions de téléchargement sur le site Web ; les opérateurs de réseaux et les FAI devraient en outre lancer des programmes permettant de gérer et de suivre le nombre de solutions installées.

4. ÉDUCATION DU CONSOMMATEUR

Les opérateurs de réseaux et les FAI devraient s'engager dans des programmes d'industrie conjointement avec les ONG et prendre leurs propres initiatives pour une éducation appropriée (par ex. campagnes d'information sur leur propre site Web).

Ces programmes doivent informer exhaustivement des menaces en relation avec la publication de données, la publicité ciblée, la piraterie et le comportement en ligne d'une manière générale (y compris ce que sont le harcèlement, la sollicitation ou les contenus inacceptables).

L'éducation doit être faite de manière ciblée avec des messages spécifiquement adaptés aux groupes d'utilisateurs respectifs, y compris aux parents et enfants. Le programme pour parents devrait se concentrer sur la question de savoir comment surveiller les activités des enfants et favoriser la prise de conscience des menaces provenant de l'environnement – de même qu'il devrait montrer aux parents les outils dont ceux-ci disposent pour gérer l'environnement en ligne de leurs enfants. L'éducation des enfants devrait se concentrer sur la reconnaissance et la gestion des menaces.

5. RÉGULATION

Les opérateurs de réseaux et les FAI doivent encourager les instances de régulation à mettre l'accent sur des domaines spécifiques d'action afin de soutenir les efforts de l'industrie visant à établir la confiance de manière proactive dans des domaines clairement situés hors des attributions et activités des fournisseurs de services (comme l'établissement de listes noires des contenus illégaux ou la mise en application de lois). Les régulateurs devraient prendre soin de ne pas instaurer des réglementations obligatoires de manière proactive dans ces domaines à moins que l'adéquation de telles mesures soit assurée.

En réponse, l'industrie doit démontrer qu'elle prend la Confiance Numérique au sérieux en prenant l'initiative de développer des solutions cohérentes. Ces solutions doivent obtenir le soutien de tous les acteurs et doivent répartir de manière proportionnée les coûts d'implémentation et les retombées financières positives qui en résultent. Les régulateurs doivent autoriser l'industrie à développer de telles solutions, promouvoir la coopération des parties prenantes et les programmes de soutien financier, en autorisant la pression concurrentielle afin de favoriser le respect des intérêts des consommateurs plutôt qu'en appliquant une régulation qui, malgré ses bonnes intentions, pourrait s'avérer en réalité contre-productive du point de vue du consommateur et entraîner un dommage économique. Par exemple, notre analyse démontre qu'une régulation stricte de la qualité du service interdisant la majorité des formes de gestion du trafic pourrait faire augmenter les dépenses d'investissement nécessaires des opérateurs de réseaux à hauteur d'un montant pouvant atteindre 6 milliards d'€ pour l'Europe.

Pour l'exécution des mesures correspondant à ces cinq domaines d'initiative, les opérateurs de réseaux et les FAI ont généralement tout intérêt à coopérer le plus possible avec les ONG. De nombreux aspects peuvent être abordés de manière nettement plus efficace lorsqu'un fournisseur prend l'initiative conjointement avec une ONG, étant donné que cette dernière peut assurer la neutralité et l'applicabilité à l'échelle de l'industrie en mettant à profit la bonne réputation générale des ONG. Des enquêtes récentes ont montré que les ONG bénéficient d'un degré élevé de confiance de la part des consommateurs.

PRIORITÉS POUR LES RÉGULATEURS

Les régulateurs et les instances gouvernementales ont à définir leur position dans cette sphère, en trouvant un équilibre entre la censure et l'éducation du consommateur, la régulation sévère et les philosophies d'autorégulation du marché libre. La nature transfrontalière des menaces envers la Confiance Numérique met particulièrement l'accent sur l'importance de la coopération internationale (judiciaire), de la prise de conscience accrue de l'urgence de l'action et, pour le gouvernement et les autorités exécutives, de l'affectation de ressources appropriées afin d'établir des structures efficaces de mitigation et des partenariats avec l'industrie. Jusqu'à présent, l'absence d'une approche cohérente va finalement au détriment du consommateur qui déplore un manque de transparence et d'assistance en ce qui concerne les risques et bénéfices de l'économie numérique, tandis que les professionnels doivent relever le défi de créer de nouveaux modèles économiques durables pour la sphère du numérique.

Il semble y avoir, dans la politique en général et dans les politiques de régulation, une tendance forte à la coopération et à la corégulation des parties prenantes plutôt qu'à une l'activité législative. En même temps, il sera nécessaire de reconsidérer en permanence l'adéquation de toute activité régulatrice, notamment en cas d'approches fortement interventionnistes (telles que la « riposte graduée » ou les démarches visant à imposer un filtrage obligatoire du réseau) qui sont susceptibles d'empiéter sur les libertés fondamentales de l'Internet, sur les droits fondamentaux du consommateur (par ex. à la vie privée) et d'ébranler les certitudes légales acquises aux yeux des acteurs de l'industrie.

Indubitablement, les régulateurs ont un rôle important à jouer pour garantir la Confiance Numérique. Étant donné la grande complexité des problèmes ayant une incidence sur la Confiance Numérique, le rôle des régulateurs visant à encourager une coopération accrue des parties prenantes pourrait être un moyen important pour parvenir à cette fin. Sur la base de l'analyse du présent rapport, les domaines suivants méritent l'attention continue des régulateurs :

• Encourager les opérateurs de réseaux et les FAI à mettre en place des politiques et procédures de la Confiance Numérique ainsi qu'une autorégulation basée sur des codes de conduite au niveau industriel – en particulier dans les domaines où une intervention plus importune serait susceptible d'entraîner des résultats économiques négatifs (par ex. la gestion du trafic) ou d'empiéter sur les droits fondamentaux des consommateurs (par ex. la règle « riposte graduée ou vous êtes dehors »).

• Considérer des mesures visant à limiter le risque juridique des opérateurs de réseaux et des FAI et, dans certains cas, le risque touchant leur réputa-tion en introduisant des politiques et procédures de Confiance Numérique, par ex. mener le développement et encourager le déploiement dans toute l'industrie d'un registre des sites interdits dans l'intérêt de la protection des mineurs – et harmoniser en Europe les approches actuellment dispersées des différents pays, ceci incluant la mise en place de structures permettant des procédures coordonnées sur le plan international pour la protection des mineurs.

• Créer des stimulants pour les acteurs de l'industrie afin de leur faire adopter un rôle plus actif dans l'éducation des consommateurs – fournir des financements et mettre en place des initiatives de coordination pour un effet amplifié, par exemple en se fondant sur les expériences acquises par le Programme pour un Internet plus Sûr (Programme Safer Internet).

• Accroître les efforts de coopération internationale pour développer des solutions globales ou des structures de résolution des problèmes globaux essentiels, par ex. dans le domaine de la protection des copyrights.

• Mettre spécialement l'accent sur les interdépendances entre les différents domaines de la Confiance Numérique pour les différentes parties prenantes et équilibrer les décisions en conséquence. Par exemple, la mise en application d'exigences très strictes concernant la qualité du service pourrait avoir des conséquences non souhaitées telles que l'entraînement de coûts considérables pour l'industrie en raison de mises à jour des réseaux, ce qui pourrait finalement provoquer une augmentation des coûts pour le consommateur.

En résumé, la Confiance Numérique ne doit pas être nécessairement chère – en termes d'investissements requis – pour être réussie. Par contre, le coût de son échec serait substantiel. Cela dit, il n'est pas nécessairement facile de faire fonctionner un programme de Confiance Numérique, et cela n'est pas complètement gratuit non plus. La plupart des PDG pensent que leurs organisations sont engagées dans un grand nombre d'activités parmi celles évoquées ci-dessus – à juste titre. Mais dans la majorité des cas, cela ne suffira pas. La Confiance Numérique dépasse largement le fait de mettre du matériel éducatif à disposition sur le site Web. Il s'agit de s'engager à un niveau supérieur avec les principales institutions privées ou publiques dans ce domaine et de lancer des campagnes sérieuses qui font la différence. Ceci nécessitera un financement et, le cas échéant, de nouvelles compétences dans les organisations. La Confiance Numérique ne se limite pas à la nécessité de posséder une politique de protection de la vie privée et des données sur fichier, il s'agit bien plus de changer la manière de penser d'une entreprise et sa manière de communiquer ces thèmes en interne, à ses clients et au public en général. En bref, la Confiance Numérique a besoin d'être menée par le haut afin de prévaloir.

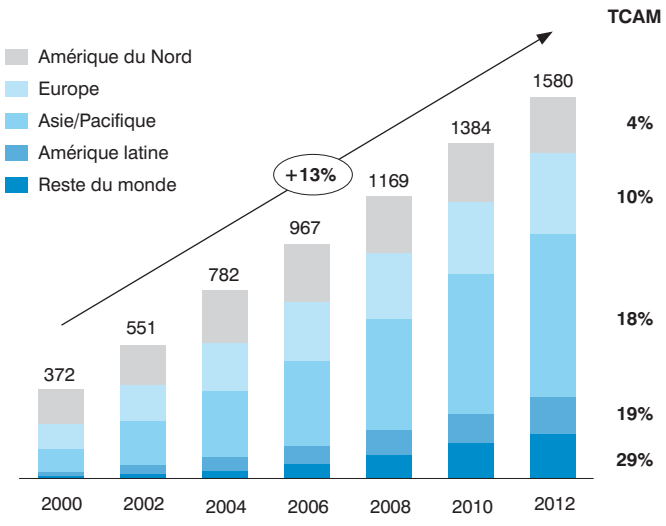
II. LA PROCHAINE VAGUE DE CROISSANCE DANS L'ÉCONOMIE NUMÉRIQUE : C'EST L'USAGE QUI MÈNE LA CROISSANCE ET NON LE NOMBRE D'UTILISATEURS

1. VIE NUMÉRIQUE : INTRODUCTION

Les technologies numériques ont révolutionné la vie de tous les jours – au bureau comme à la maison – à la vitesse de l'éclair. Les cycles de développement en ralentissement et, en résultat, des dispositifs de plus en plus puissants combinés à des cycles technologiques de remplacement introduisant des raccourcis drastiques entraînent une pénétration massive du marché par la technologie numérique. Que ce soit au niveau de la connexion et de la communication entre amis, pour regarder des films, écouter de la musique ou prendre des photos, la vie est aujourd'hui numérique. Les technologies numériques sont depuis longtemps sorties de leur niche en tant que jouets uniquement destinés aux férus de technologie pour devenir l'avant-plan et le centre de la vie moderne. La majorité des consommateurs d'aujourd'hui sont plus embarrassés lorsqu'ils perdent leur connexion Internet à la maison que lorsqu'ils perdent leur ligne téléphonique.

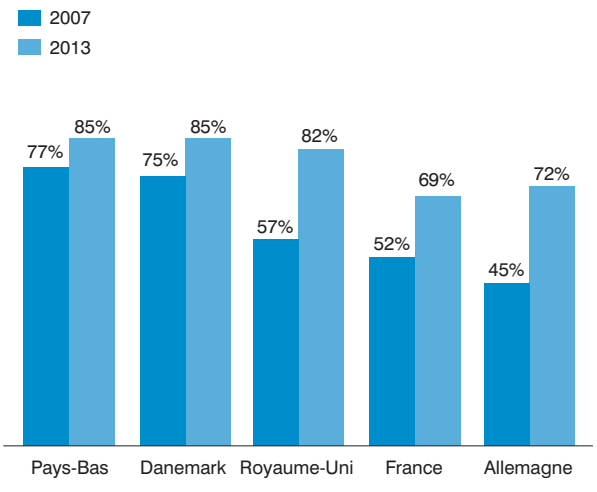
Le développement le plus récent des services numériques, allant de la télévision numérique aux applications dites Web 2.0, a clairement démontré que le plein potentiel de la technologie et des services numériques ne peut être atteint que si les technologies et applications sont connectées physiquement et logiquement en réseau. Quelle est la véritable révolution au sein de la photographie numérique ? Le fait que la pellicule celluloïd ait disparu des étalages, ou le fait que les photos puissent aujourd'hui être partagées et échangées en quelques minutes entre amis, juste après leur prise ? Les applications Web 2.0 plus particulièrement, telles que Facebook et YouTube, qui mettent très fortement l'accent sur l'aspect de communauté de la technologie numérique, soulignent nettement ce point. Lorsque la communication, la communauté, le contenu et le commerce sont combinés, la valeur ajoutée est immense pour le consommateur – et profondément innovatrice à de nombreux égards. Les taux de croissance exponentiels de ces services dans toutes les économies occidentales et au-delà en sont le témoignage expressif. Il est assez intéressant de constater que tous ces services tirent un avantage immédiat de cet aspect communautaire : le marketing viral, c'est-à-dire la communication orale ou d'ordinateur à ordinateur est leur principal facteur de croissance. Tout ceci n'est possible que dans un environnement connecté en réseau.

Illustration 1 : Utilisateurs Internet, monde (millions d'utilisateurs)



Source : Economist Intelligence Unit

Illustration 2 : Pénétration du haut débit (% des ménages)



Source : OECD

Dans ce contexte, il est important de noter que la majorité des ménages européens est déjà ou sera bientôt équipée de trois connexions numériques en réseau : Internet, télévision numérique et mobile. Ceux-ci étant tous en mesure, à différents degrés, de fournir des services haut débit et étant tous, encore à différents degrés, interactifs.

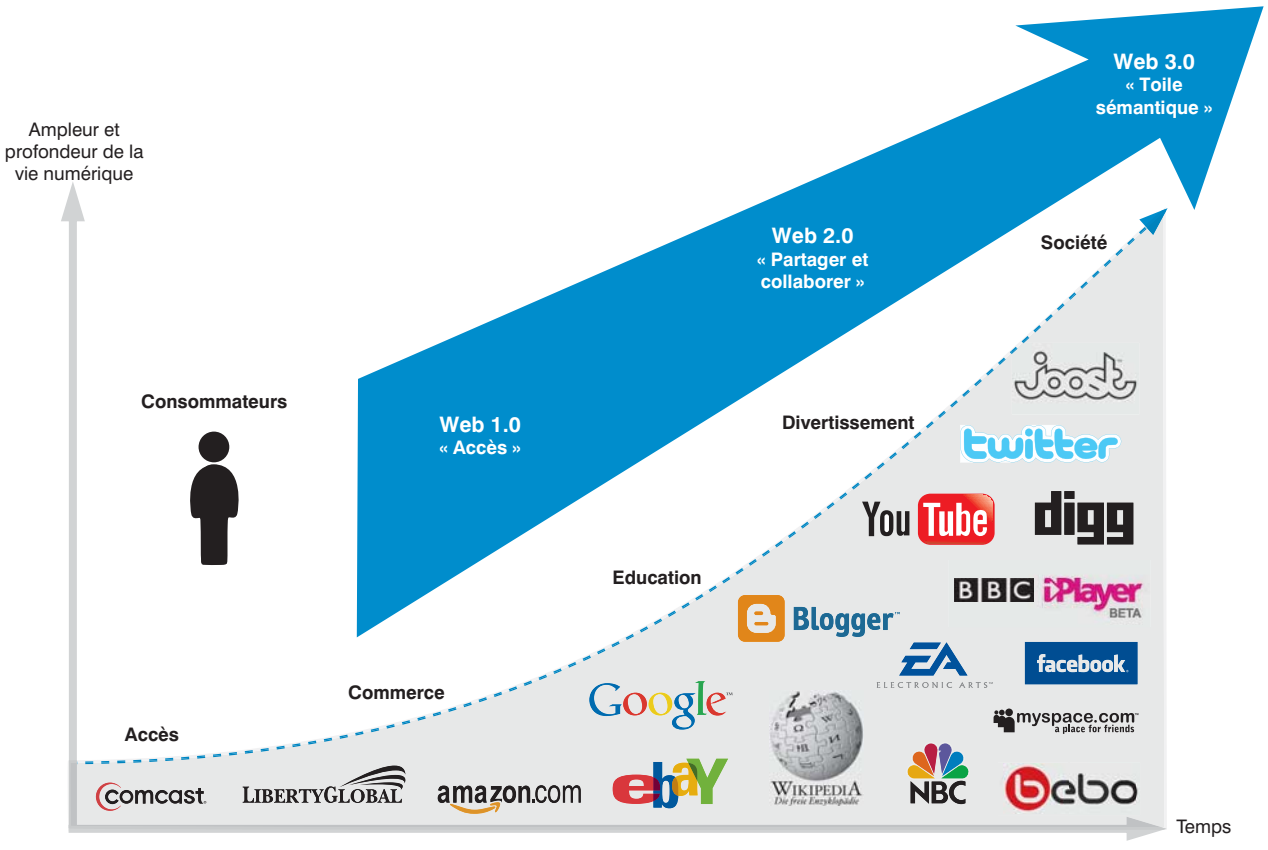
Les niveaux de pénétration Internet et haut débit atteignent désormais la saturation, la pénétration a atteint 70 % dans la majorité des marchés européens centraux.

La migration actuelle des réseaux haut débit vers des accès réseau nouvelle génération accélèrera encore plus le développement de l'économie numérique. Les réseaux câblés de la prochaine génération (basés sur la technologie EuroDOCSIS 3.0), les acteurs télécommuni-cations (xDSL), les opérateurs de téléphonie mobile et les fournisseurs de réseau local FTTH, combinés aux ensembles sans fil tels les réseaux numériques terrestres et satellites, pourvoiront à la demande en termes de haut débit à des vitesses supérieures, de connectivité omniprésente et de consommation média individualisée par le biais de platesformes.

La disponibilité et le niveau d'acceptation de l'Internet sont tels que la pénétration du haut débit est supérieure à 70 % dans de nombreux pays européens et a acquis le statut d'un phénomène de marché de masse, comparable à d'autres formats de médias tels que la télévision et la radio. Ce fait oriente également la prochaine vague de changement dans le comportement des consommateurs qui sont de plus en plus nombreux à exiger l'accès au service de leur choix, en temps et lieu de leur choix et en utilisant le dispositif disponible.

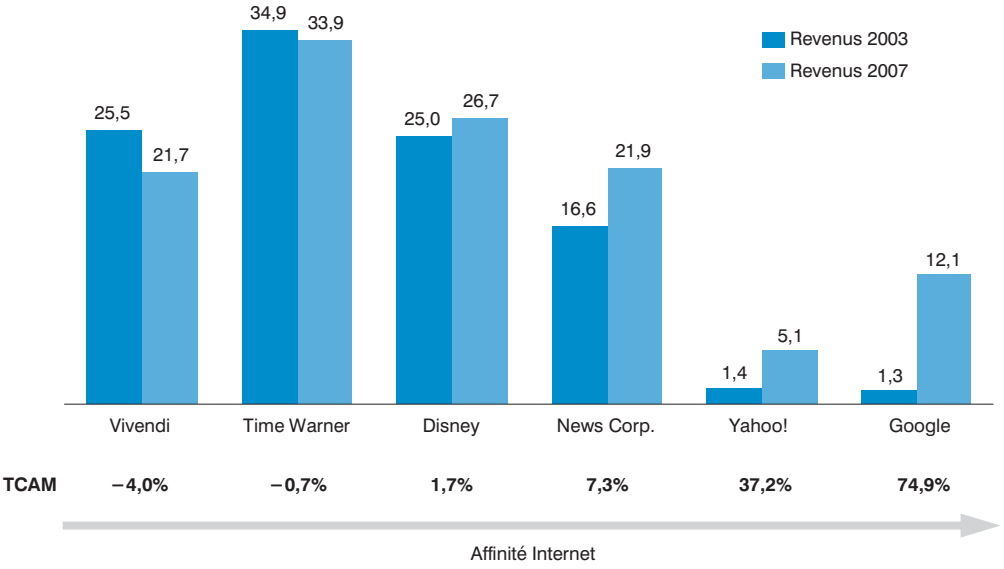
Les consommateurs modifient les modèles de comportement, non seulement en passant plus de temps en ligne, mais également en interagissant plus en ligne – par l'intermédiaire de réseaux sociaux qui fournissent aux utilisateurs l'opportunité d'échanger des pensées, des contenus et des idées. Du côté des fournisseurs, la comparaison entre les entreprises de médias plus traditionnelles et les nouveaux géants numériques montre très clairement où s'est trouvée la croissance au cours de ces dernières années (Illustration 4). Et même au sein des compagnies de médias plus traditionnelles, ce sont les plus impliquées en ligne qui grandissent le plus rapidement : News Corp. aux fortes activités numériques telles que MySpace en est un bon exemple.

Illustration 3: *Développement de la vie numérique*



Source : Booz & Company

Illustration 4 : Comparaison entre sociétés des médias et sociétés de l'Internet (revenus en milliards d'euros)



Source : OneSource, rapports annuels

2. VIE NUMÉRIQUE : UNE FORCE DE DÉFINITION DE L'ÉCONOMIE, DE LA POLITIQUE, DE LA SOCIÉTÉ ET DE L'ÉDUCATION D'AUJOURD'HUI

Jusqu'ici, la croissance de la consommation Internet a été largement entraînée par la sortie de nouvelles technologies. L'équipement des utilisateurs finaux, tel que les ordinateurs et les dispositifs mobiles, permet un accès et des platesformes de stockage économiques. Les réseaux haut débit sont en train d'évoluer vers les réseaux ultrarapides de la prochaine génération. Toutes les infrastructures pertinentes fournissent de hautes capacités (offres haut débit standard fournissant environ 5 Mbps et, dans les pays plus développés, jusqu'à 25 ou même 100 Mbps) combinées à des aptitudes interactives et à une fonctionnalité de marche en permanence. En effet, les ORM (opérateurs de réseaux mobiles) ont finalement introduit l'Internet mobile avec une disponibilité généralisée de réseau 3G à travers l'Europe.

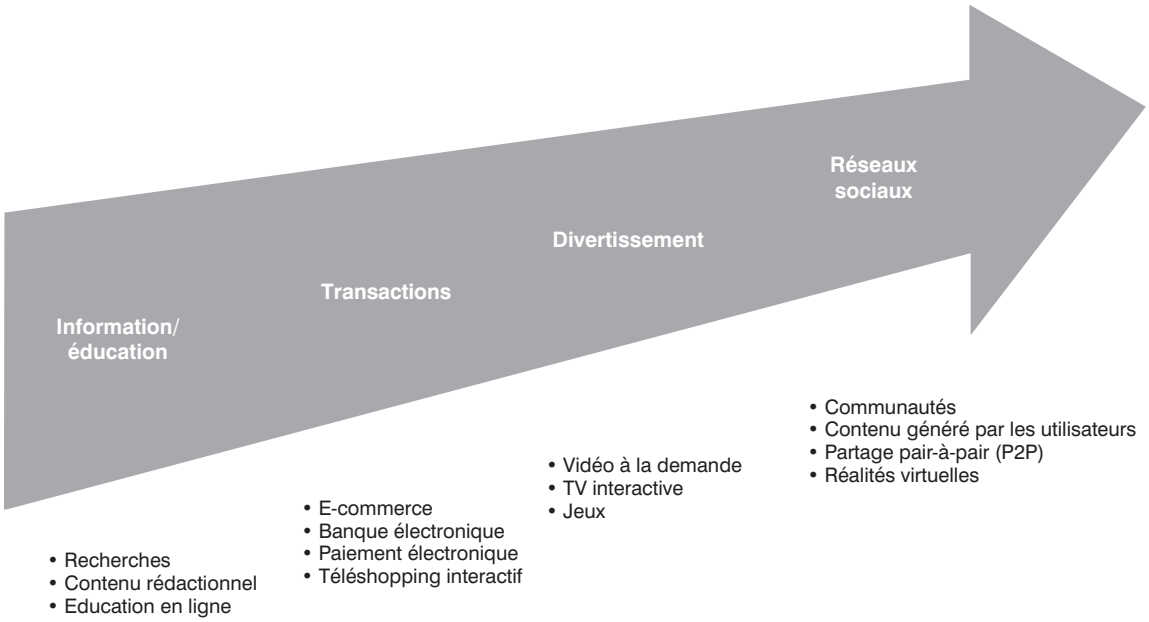
Les producteurs de technologie actuels ont amené les niveaux de pénétration des accès à Internet à la quasi saturation sur de nombreux marchés. Ainsi, la prochaine vague de croissance numérique sera portée par l'exploitation des technologies en vue d'atteindre une ampleur nettement supérieure bien plus que pour approfondir leur pénétration. Ceci implique un changement dans l'usage ou dans le comportement de l'utilisateur bien plus qu'une augmentation du nombre d'utilisateurs. Et c'est ce que nous observons, aujourd'hui déjà, sur de nombreux marchés. Le comportement des consommateurs est en train de changer de manière radicale : la principale source d'information influençant la décision d'achat d'une voiture est l'Internet ; un livre sur deux vendu aux Etats-Unis aujourd'hui est vendu en ligne par Amazon et l'opérateur câble Comcast basé aux Etats-Unis enregistre 40 millions de téléchargements de films à la demande par mois.

En réponse aux changements dans les modèles de consommation de médias, les entreprises ont recours à la puissance de l'Internet pour leur publicité et à des fins de marketing : au Royaume-Uni par exemple, plus de 15 % des dépenses de publicité sont allouées aux médias en ligne.

L'Internet et l'environnement numérique en général se sont développés pour devenir une plateforme très séduisante pour diverses activités de publicité et de marketing : premièrement, les consommateurs consacrent de plus en plus de temps aux médias numériques, et deuxièmement – point absolument crucial – les médias numériques ont une efficacité énorme et des avantages considérables par rapport aux autres formats publicitaires. De nombreuses approches publicitaires sophistiquées, en particulier celles visant à accroître leur pertinence vis-à-vis du consommateur individuel, peuvent seulement être déployées du fait que le média numérique peut exploiter une grande profusion d'informations sur les utilisateurs et l'usage.

L'Internet est à l'origine des changements subis par les industries – Amazon vend des livres pour plus de 4,5 milliards de $ aux Etats-Unis, représentant près d'un livre sur deux vendus en ligne, comparable à Barnes&Noble dans les ventes traditionnelles.

Illustration 5 : Vie numérique—sources de croissance

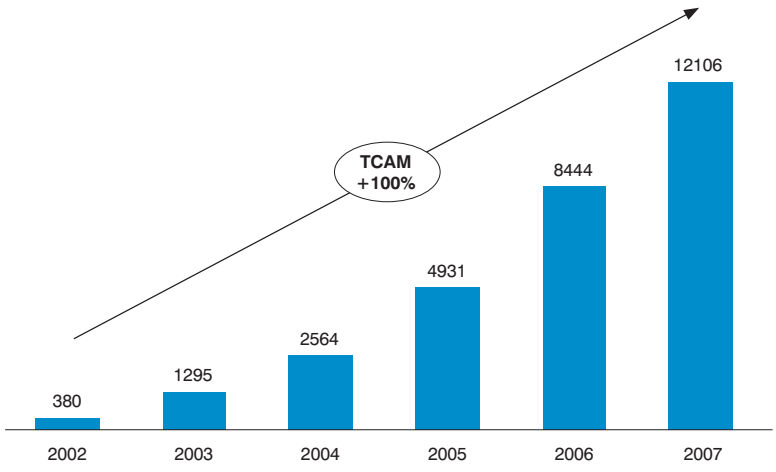


Par exemple, les utilisateurs de l'offre e-mail de Google appelée Gmail reçoivent une publicité taillée sur mesure en fonction du contenu de leurs e-mails. De la même manière, l'historique de navigation en ligne, les profils administrés activement et autres données peuvent être utilisés pour adapter une publicité adressée à des consommateurs individuels. Avec la télévision numérique également, les données de l'utilisateur et les données concernant son usage peuvent être suivies par le biais d'un décodeur et utilisées pour présenter une publicité ciblée à des segments spécifiques ou à des utilisateurs individuels ; avec la télévision numérique interactive, la publicité offre les mêmes caractéristiques de réponse interactive qu'Internet.

Les annonceurs consacrent désormais une plus grande part de leurs dépenses à l'Internet – la publicité en ligne représente 15 % de la publicité totale au Royaume-Uni.

La garantie d'un niveau élevé de protection de la vie privée est un aspect très important du point de vue du consommateur qui doit être considéré avec une grande précaution, même si les données du trafic Internet de l'utilisateur sont utilisées à des fins commerciales à des niveaux regroupés et anonymes. Mais aussi importun que ceci puisse paraître à première vue, l'expérience montre que la publicité adaptée est en mesure d'accroître l'acceptation par le consommateur lorsqu'elle est bien réalisée, car la publicité est alors pertinente pour le consommateur. En outre, il existe de nombreuses façons de concevoir une telle publicité, de telle sorte qu'une participation non souhaitée peut être évitée : par le biais de procédures opt-in ou opt-out par exemple, il est possible pour les utilisateurs de décider que leurs données ne soient pas utilisées pour une publicité ciblée – mais dans ce cas, il se peut également que les utilisateurs ayant fait ce choix soient de plus en plus souvent appelés à payer pour certains services afin de compenser la perte de recettes publicitaires. Qui plus est, la publicité restera l'un des principaux moyens de financement pour un grand nombre de services et d'offres dans l'environnement numérique, de même qu'elle a été le moyen de financement des médias traditionnels pendant des décennies.

Illustration 6 : Croissance de Google (revenus en millions d'euros)



Source : Google

Sur cette toile de fond et avec l'expérience des quinze dernières années dans le domaine de l'économie numérique, il est fort probable que la publicité au sens large devienne l'une des principales sources de revenus venant soutenir la croissance future de l'économie numérique. La gestion de l'intrusion - réelle ou perçue - sur Internet est néanmoins un préalable incontournable pour s'emparer de cette croissance. Notamment au regard de la pression accrue incitant à monétiser les nouveaux services du Web 2.0, ceci sera l'un des plus grands défis pour tous les acteurs impliqués de l'industrie.

Dans la perspective de l'application, nous distinguons principalement quatre leviers de croissance de l'économie numérique :

- **Information et éducation :** applications traditionnelles du Web 1.0 combinées avec certaines petites modifications du Web 2.0 telles que les contenus générés par des utilisateurs, par exemple par un apprentissage en ligne.

- **Services transactionnels :** principalement le e-commerce et la banque en ligne.

- **Divertissement :** télévision numérique, services vidéo (streaming de vidéos et offres de vidéo à la demande telles que YouTube), jeux ou encore services de téléchargements tels que iTunes.

- **Réseaux sociaux :** tous services bâtis autour de l'interaction entre individus, par exemple dans les communautés, l'échange de contenus – principalement générés par eux-mêmes – ou les rencontres au sein de réalités virtuelles.

INFORMATION ET ÉDUCATION

L'information – et en particulier la recherche – ont été l'un des principaux facteurs de croissance de la consommation Internet depuis le commencement de celui-ci. Les moteurs de recherche ont atteint un succès notable en accomplissant la traduction de quantités infinies de données disponibles aujourd'hui sur le Web en une information significative et structurée pour les utilisateurs finaux.

L'Internet facilite par ailleurs la collaboration, fournit des enseignements aux consommateurs grâce à des idées et des contenus générés par les utilisateurs, par exemple Wikipédia qui rassemble plus de 10 millions d'articles générés par les utilisateurs dans 250 langues. Lancé en 2001 seulement, Wikipédia est en train de devenir la source d'information (encyclopédique) la plus demandée en termes d'accès – non pas uniquement parmi les offres Internet mais parmi la totalité des sources d'information disponibles. Wikipédia est ainsi en train de devenir l'un des outils d'éducation et de recherche les plus importants – et va même jusqu'à provoquer des discussions au sujet des étudiants qui perdent la faculté de faire de « vraies » recherches documentaires en bibliothèque. La nature ouverte et communautaire de Wikipédia, aussi bien pour ce qui est de ses contenus générés par les utilisateurs qu'en raison de son contrôle des utili-sateurs, en fait un exemple primordial des véritables applications Web 2.0 entrant dans la sphère de l'information. Selon certains, sa nature dynamique serait à même de fournir plus d'exactitude que de nombreuses autres sources d'information plus statiques.

Plus de 45 % des entreprises utilisent régulièrement des entraînements basés sur l'Internet.

La télévision numérique est un autre facteur majeur de l'ère de l'information. Le nombre de chaînes télévisées diffusées en Europe a atteint la quantité prodigieuse de 1.703 chaînes (en 2005) après un démarrage avec 93 chaînes il y a à peine 18 ans. Un grand nombre de ces chaînes aujourd'hui disponibles pour les consommateurs se consacre aux informations, aux documentaires ou aux langues étrangères, ce qui était soit inexistant soit inaccessible auparavant dans l'univers analogique.

Les universités et les autres institutions d'enseignement supérieur tirent de plus en plus profit des possibilités fournies par Internet pour distribuer l'information de manière très efficace et pour permettre une interaction commode et riche, avec le soutien de solutions telles que WebEx (une solution de conférence et de collaboration Web). En particulier, l'enseignement à distance qui était encore tributaire d'un grand nombre de transports physiques il y a quinze ans (voyages des personnes, exercices et devoirs envoyés par courrier) utilise aujourd'hui pleinement ces possibilités. Plusieurs universités et collèges (l'Open University au Royaume-Uni par exemple) ont commencé à s'engager dans Second Life pour en tirer profit comme environnement virtuel d'enseignement. De même, les entreprises emploient l'Internet et les médias numériques associés afin de proposer des entraînements à leurs salariés, en employant des formats tels que les Webcasts ou l'entraînement basé sur le Web (web-based training, WBT), qui est un élargissement du traditionnel entraînement basé sur ordinateur (CBT).

L'information et l'éducation continueront à être d'importants leviers de croissance pour l'économie numérique. En particulier, la recherche soutenue par la publicité en ligne

maintiendra une forte croissance. Google, l'exemple par excellence en ce qui concerne la traduction des recherches effectuées en recettes publicitaires, a pu se réjouir d'une croissance annuelle de ses revenus de plus de 100 % au cours des cinq dernières années en appliquant ses modèles économiques de manière dynamique et en continuant à innover dans ses offres, atteignant desormais plus du double de la taille du diffuseur Européen leader RTL Group.

TRANSACTIONS

L'Internet a prouvé être un moyen idéal pour les activités transactionnelles.

Lorsqu'ils font du shopping en ligne, les consommateurs apprécient les prix compétitifs plus que bien d'autres avantages, en faisant appel à cette occasion aux sites de comparaison des prix. Aujourd'hui, avec plus de 40 % de consommateurs faisant leurs achats en ligne, les dépenses annuelles effectuées dans le e-commerce constituent un excédent de 150 milliards d'€ en Europe, avec une croissance de 50 % sur les deux dernières années. Ces dépenses effectuées dans le e-commerce aujourd'hui représentent plus de 4 % du total des ventes au détail en Europe, et il est prévu qu'elles atteignent 11 % en 2011. Pour certains produits comme les billets d'entrée à des manifestations, les voyages et les médias (livres, musique, vidéos et logiciels), la part en 2011 est prévue entre 25 % et 35 %.

Plus de 40 % des consommateurs font du shopping en ligne, et le e-commerce représente aujourd'hui plus de 4 % du total des ventes au détail en Europe.

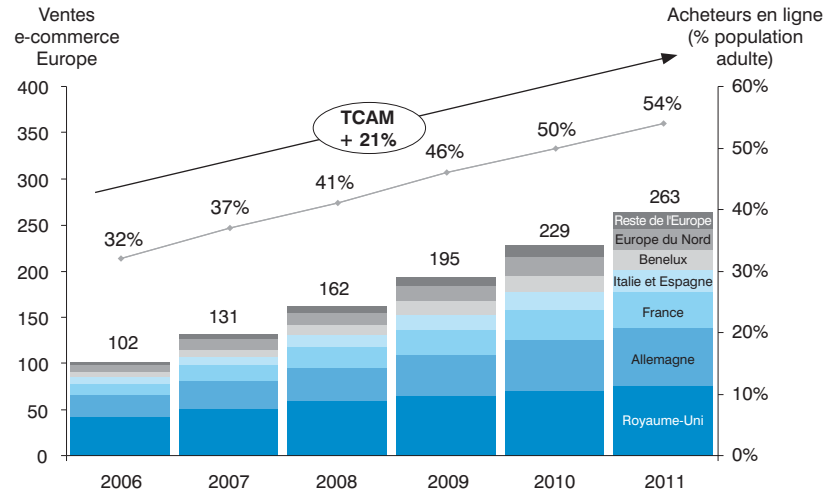
En outre, l'Internet a également révolutionné la manière dont les consommateurs gèrent leurs finances en leur permettant d'effectuer leurs transactions numériquement. Étant donné que l'Internet a réussi à établir un niveau significatif de confiance en sa sécurité (qui s'avère globalement solide), l'utilisation de la banque électronique s'est développée pour devenir un phénomène de masse. Et à côté de la croissance du e-commerce, une large palette de solutions de paiement électronique telles que PayPal a su s'établir pour apporter un soutien à l'intérêt croissant porté aux achats de biens et services en ligne. En raison cependant de la sensibilité particulièrement élevée entourant les transac-tions financières, il est évident que ces domaines sont éminemment exposés aux problématiques de sécurité.

De nouvelles entreprises se sont établies sur la base de modèles uniquement tournés vers l'Internet, tirant avantage de l'opportunité d'appliquer un modèle économique virtuel pour une fraction des coûts d'une entreprise issue de l'économie réelle ; elles tirent profit de la puissance de l'Internet en tant que canal de vente low-cost permettant une gestion efficace de la chaîne d'approvisionnement. Les entreprises issues de l'économie réelle profitent, elles aussi, d'une plateforme low-cost supplémentaire pour le service clientèle et les opérations de facturation – et font fréquemment payer un supplément aux utilisateurs refusant d'utiliser le service Internet. Les opérateurs de téléphonie mobile par exemple ont introduit, il y a quelques années déjà, des offres uniquement disponibles sur Internet.

DIVERTISSEMENT

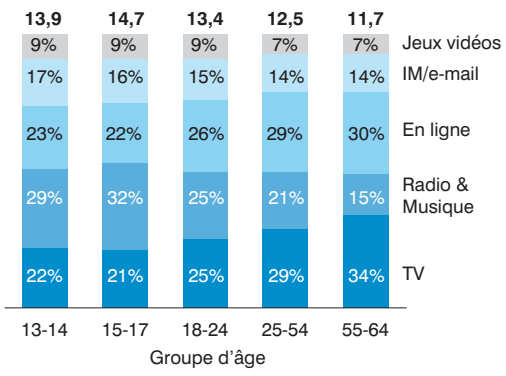
Le changement probablement le plus profond apporté par l'économie numérique à la majorité des consommateurs se situe dans le domaine

Illustration 7 : Ventes au détail e-commerce en Europe (milliards d'euros)



Source : Forrester

Illustration 8 : Temps passé avec les médias par jour (heures par jour, 2007)



Source : eMarketer

du divertissement. Le consommateur européen moyen passe entre 160 et 240 minutes par jour devant la télévision. Et il passe jusqu'à 140 minutes supplémentaires sur Internet – de plus en plus à des fins de divertissement. Comptabilisés ensemble, l'usage et la consommation de médias interactifs sont de loin l'activité de loisir numéro un en Europe en termes de temps. Et cette situation est en train de changer de manière radicale. L'Internet est d'ores et déjà en train de devenir le média en tête dans de nombreuses économies développées, avec des individus passant plus de temps en ligne ou en correspondance e-mail que devant la télévision (Illustration 8).

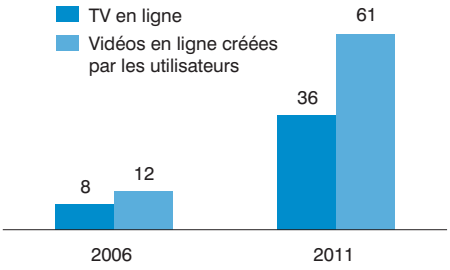
Du fait de leurs emplois du temps de plus en plus chargés, les consommateurs ont tendance à se tourner vers des services de divertissement à la demande qui leur permettent de regarder ce qu'ils veulent quand ils le veulent et comme ils le veulent. Les capacités accrues des réseaux haut débit permettent de fournir de manière rentable et économique des services tels que la vidéo à la demande.

La télévision numérique est en passe de révolutionner le vécu TV des consommateurs. Les dernières années ont été accompagnées d'une véritable explosion du nombre et de la diversité des chaînes de télévision, avec une augmentation importante du nombre de chaînes régio-nales ou thématiques. En outre, les évolutions techniques permettent une qualité d'image nettement supérieure avec les offres HDTV. La télévision numérique a également introduit un certain nombre de fonctionnalités entièrement nouvelles telles que la vidéo à la demande, la télévision en différée ; par ailleurs, elle soutient aussi des fonctions spéciales telles que l'interactivité ou des guides de programme électroniques supplémentaires.

En outre émergent des langages et des platesformes commerciales qui tirent avantage des capacités accrues des réseaux haut débit pour fournir des services multimédias sur Internet – par exemple, le iPlayer de la BBC propose des émissions TV et radio sur Internet au Royaume-Uni.

Plus de la moitié des utilisateurs d'Internet aux États-Unis (57 %) ont déjà utilisé l'Internet pour regarder des vidéos en ligne, et presque 20 % des consommateurs le font tous les jours. Et ces pourcentages sont encore plus élevés chez les utilisateurs disposant de connexions haut débit (74 % d'entre eux regardent des vidéos en ligne). L'année dernière, quelques start-ups dotées d'une grande agilité ont commencé à faire de l'Internet une véritable télévision : Joost, Babelgum et d'autres sont en train de déployer des offres de télévision haute qualité enrichies de fonctionnalités Web 2.0 selon une méthode dite « over-the-top » (OTT), c.-à-d. « au sommet » d'un réseau câble ou d'un réseau d'opérateur télécoms sans aucune liaison avec le fournisseur de réseau.

Illustration 9 : Flux vidéos en ligne aux Etats-Unis (milliards de transmissions vidéos)



Source : eMarketer

Ces tendances ne se limitent pas seulement à accroître l'importance de l'Internet en tant que média pour la publicité ; elles sont également en train de l'établir comme étant un moyen important pour forger l'opinion publique, un moyen auquel les défenseurs de la liberté d'opinion et un public bien informé (politique, sciences sociales et institutions culturelles) témoigneront un intérêt accru dans le cadre de tels changements concernant la consommation de médias.

RÉSEAUX SOCIAUX

La société est en train de connaître des niveaux supérieurs d'interaction grâce à des sites de réseaux sociaux tels que Facebook et Bebo qui, d'un côté, ont apporté des fonctionnalités qui seraient restées impossibles sans Internet et qui permettent aux individus de vivre des amitiés en ligne n'étant aucunement préjudiciées par la distance physique, mais qui, de l'autre côté, font également grandir certaines craintes quant à la destinée des comportements sociétaux traditionnels tels que l'interaction et l'amitié en face à face.

Le comportement social est en train de changer – les gens se connectent plus rapidement et avec des groupes sociaux de plus grande taille lorsqu'ils utilisent l'Internet.

Les réseaux sociaux en ligne sont un phénomène relativement récent qui soutient la tendance Web 2.0 générale se dirigeant vers des communautés sociales en ligne. Les utilisateurs – en particulier ceux de la génération « née à l'ère du numérique » – font partie des groupes d'intérêts sociaux qui agissent dans un contexte en ligne et qui génèrent, envoient et partagent des contenus en ligne. Les réseaux sociaux sont utilisés par une part croissante d'internautes, dont la majorité accède à de multiples sites de manière régulière.

La génération 'née à l'ère du numérique' — Faire avancer la Confiance Numérique

Les enfants et les jeunes des pays industrialisés sont la première génération née dans un monde numérique. Ils sont des adopteurs précoces des nouvelles technologies et des experts en informatique, comparés à la plupart des parents. Et jusqu'à présent, seule une partie des généra-tions plus âgées a vécu une « renaissance » dans cette vie numérique.
Le magazine Wired écrit au sujet des jeunes « nés à l'ère du numérique » :

- Une auto-caractérisation: « Nous avons appris à marcher autour de l'ordinateur. Nous avons atteint notre majorité en même temps que l'Internet. Adopteurs précoces, hyperconnectés, toujours en ligne »
- Sur la technologie : « De Messenger au MP3 et au P2P, nous testons la culture de demain. Tandis que d'autres s'émerveillent du futur numérique, nous le considérons comme allant de soi. Considérez ceci comme la différence entre une deuxième et une première langue »

La génération « née à l'ère du numérique » ne fait pas la distinction entre « en ligne » et « hors ligne » tel que de nombreux adultes ont tendance à le faire – les deux « mondes » sont nettement plus interconnectés pour eux ; ils vivent dans des communautés réelles autant que virtuelles avec une superposition fréquemment importante dans leurs groupes d'âge ; en outre, ils ont leur propre culture « en ligne », leur propre langage et leur propre « netiquette ».
Mais les membres de la génération « née à l'ère du numérique » lancent également certains défis, pour eux-mêmes aussi bien que pour le reste de la société :

- Un paradoxe considérable : ils s'exposent largement sur des sites de réseaux sociaux, renonçant ainsi délibérément à leur vie privée, mais ils réagissent violemment lorsqu'ils n'apprécient pas la manière dont sont utilisées leur données – comme dans le cas Beacon de Facebook, dans lequel plus de 50.000 utilisateurs ont signé une pétition en décebre 2007 pour se plaindre du programme destiné à intégrer Facebook à d'autres sites Web de partenaires externes à des fins de référence croisée et de publicité ciblée.
- Les parents et les écoles (les « éducateurs naturels ») sont dépassés par l'ampleur des nouveaux phénomènes et par la rapidité des innovations.
- Les valeurs et standards légaux traditionnels sont plus difficiles à appliquer à des activités numériques « ambiguës » et obtiennent une aceptation moins forte, par ex. tout autour du partage de contenus sous copyright.

Globalement, les jeunes « nés à l'ère du numérique » ne sont pas suffisamment orientés vers un comportement adéquat dans des environnements numériques – ce qui exerce une pression sur les modèles économiques : depuis de longues années déjà dans le cas du partage des contenus sous copyright, mais également à l'avenir alors que l'industrie tente de mettre en place de nouveaux modèles de publicité ciblée.

L'Internet influence depuis un temps certain le comportement social des consommateurs. Selon une étude sur les liens sociaux réalisée en 2004 aux États-Unis, c'est l'internaute moyen qui connaît un nombre plus important de personnes avec lesquelles il interagit régulièrement (37 liens sociaux pour les internautes par rapport à 30 pour les personnes n'utilisant pas l'Internet). Plus de 30 % des utilisateurs d'Internet ont en outre déclaré qu'Internet a fait croître le nombre de leurs liens sociaux et de leurs connaissances.

CHANGEMENTS DANS LA SOCIÉTÉ

Comme évoqué ci-dessus et de manière plus détaillée tout au long du rapport, la technologie numérique est une force économique majeure – elle l'est aujourd'hui déjà et elle le sera encore plus à l'avenir. Mais la limiter à un facteur purement économique serait une erreur. L'Internet en particulier et les services numériques au sens plus large seront un facteur essentiel de changement ayant un impact allant bien au-delà des ventes de livres ou de billets d'avion. Les technologies numériques permettent à chacune et à chacun de se faire entendre et d'interpeller un large public dans n'importe quel contexte pertinent pour l'individu.

L'Internet est un moyen de plus en plus important pour forger les opinions - Google est fréquemment cité comme l'une des souces d'informations globales les plus fiables, directement après CNN et BBC.

Les politiciens utilisent l'Internet pour se présenter eux-mêmes et pour présenter leurs idées, pour interagir avec les personnes qui les soutiennent et pour organiser leur campagne. Le candidat à l'élection présidentielle des États-Unis Barack Obama utilise largement les applications de réseaux sociaux dans sa campagne présidentielle. Sur l'outil Twitter, plus de 30.000 utilisateurs déclarent le « suivre » et reçoivent régulièrement de lui de brèves actualisations. Près d'un quart des Américains utilise aujourd'hui l'Internet de manière régulière comme source d'information sur la politique ou les campagnes ; dans le groupe d'âge des 18-29 ans, la part se situe à plus de 40 %. Obama a fait avancer l'utilisation de l'Internet comme outil politique vers de nouvelles sphères : il l'utilise également afin de collecter des fonds pour sa campagne. Plus d'un million de personnes ont versé en moyenne 105 $ — une possibilité encore inconnue il y a 10 ans, mais qui est devenue aujourd'hui l'une des sources de financement les plus importantes.

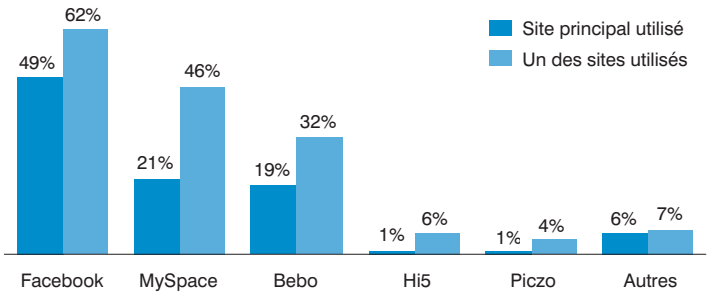
Les blogs, podcasts, sites de chat, forums d'utilisateurs, groupes de news et autres outils de communication avancée et de publication en ligne ont non seulement fondamentalement changé la communication nécessaire dans les organisations pour répondre aux objectifs commerciaux et aux autres exigences de communica-tion ; mais en rendant la communication beaucoup plus facile, ils ont également accru de manière significative la vitesse et le volume des informations et des échos échangés. L'une des conséquences de cela est que les organisations ont été confrontées à une augmentation radicale de la nécessité de concevoir et de déployer des politiques d'information et de communication, notamment en ce qui concerne les informations commerciales confidentielles. Les portails d'opinion tels que ciao – qui opère dans plusieurs pays européens et qui enregistre plus de 38 millions de visites chaque mois – et les blogs ont créé une source véritablement nouvelle d'informa-tion avant achat qui peut s'orienter soit clairement en faveur soit fermement contre des vendeurs individuels, fournisseurs de services, détaillants, etc. Le pouvoir des blogs et des « publications » en ligne va bien au-delà du pur e-commerce et du monde numérique lui-même : Kate Hanni, une passagère d'une compagnie aérienne extrêmement insatisfaite des pratiques d'American Airlines, a fondé l'association Coalition pour une Charte des Droits des Passagers des Transports Aériens avec quelques compagnons d'infortune après avoir été « bloquée dans plusieurs avions d'American Airlines pendant jusqu'à 9 heures à l'aéroport international d'Austin » en décembre 2006, sans « nourriture ni eau ni accès aux toilettes de bord en service ». L'association a maintenant plus de 20.000 membres, elle exploite un site Web et un blog pour échanger leurs « mauvaises expériences » et pour se faire entendre – et elle a été à plusieurs reprises devant le Congrès américain, déclenchant ainsi une discussion concernant des modifications de la législation et de la réglementation afin d'éviter à l'avenir les « mauvaises expériences » dont ses membres ont été victimes.

Le pouvoir des offres Web 2.0 – comme les portails d'opinion et les fonctions telles que les commentaires d'utilisateurs sur Amazon – est confirmé par le Baromètre de Confiance Edelman : l'édition 2008 montre que dans de nombreux pays comprenant les États-Unis, les Pays-Bas et l'Allemagne, « une personne comme moi » est considérée comme étant la source d'information la plus crédible au sujet d'une entreprise ou d'une société, obtenant une évaluation nettement plus élevée que n'importe quelle source d'information officielle, y compris le PDG. Dans tous les pays, quatre personnes interrogées sur cinq ont déclaré avoir « nettement plus tendance à croire ce qu'elles voient, lisent ou entendent au sujet d'une entreprise ou d'une société si quelqu'un de leur connaissance a déjà mentionné la même chose devant elles ». Du côté institutionnel, les ONG sont évaluées comme étant les plus dignes de confiance en comparaison avec les entreprises, les médias et les gouvernements – au Royaume-Uni, en Allemagne et en France, les ONG sont en tête des classements avec une avance substantielle.

La société a été remodelée par l'Internet – par exemple, 60 % des consommateurs américains seraient prêts à renoncer à leur téléphone, mais seulement 55 % à l'Internet.

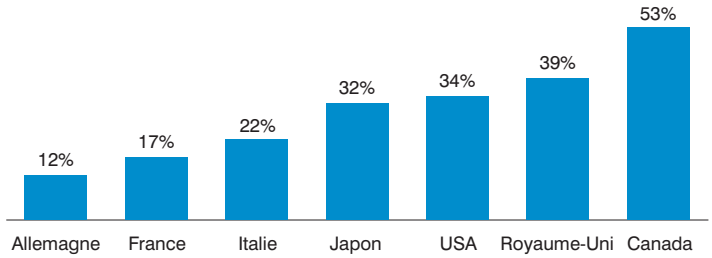
Le rythme auquel les changements se mettent en place dans le monde numérique est un rythme à couper le souffle pour beaucoup d'entre nous. En même temps, il existe une nouvelle génération « née à l'ère du numérique » pour laquelle les possibilités du monde numérique sont tout aussi ordinaires et peu spectaculaires que la radio ne l'a été pour la plupart des gens il y a 50 ans : ils sont des adopteurs précoces des nouvelles technologies et des experts en

Illustration 10 : Réseaux sociaux utilisés par les adultes (Royaume-Uni 2007, % d'utilisateurs de réseaux sociaux)



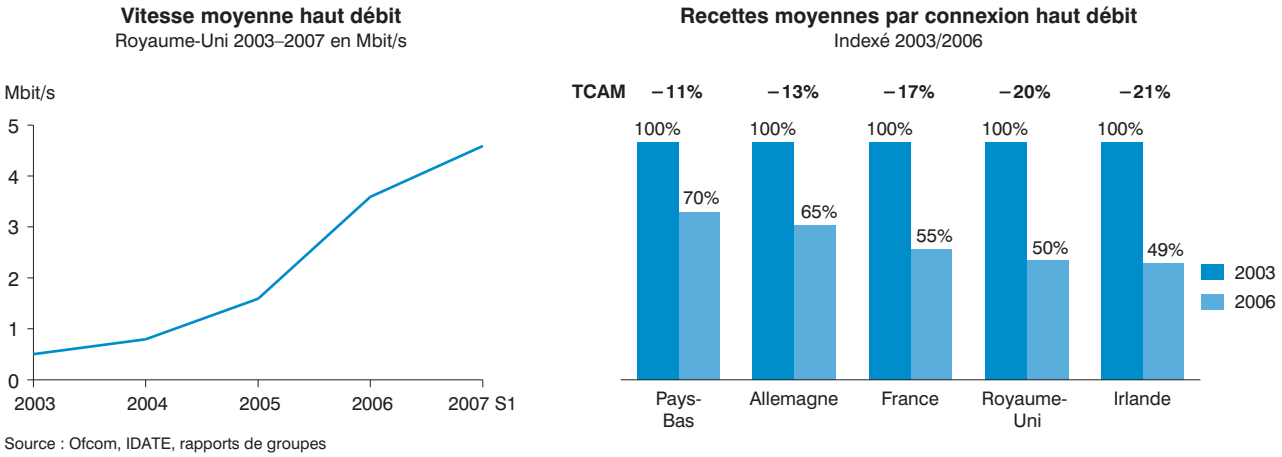
Source : Ofcom

Illustration 11 : Réseaux sociaux utilisés par les adultes (2007, % d'utilisateurs Internet par pays)



Source : Ofcom, Nielsen n=391

Illustration 12 : Dilemme de la connectivité haut débit



Source : Ofcom, IDATE, rapports de groupes

informatique, comparés à la plupart des parents ; ils ne font pas la distinction entre « en ligne » et « hors ligne » tel que de nombreux adultes ont tendance à le faire, mais ils vivent plutôt dans des communautés réelles autant que virtuelles avec une superposition fréquemment importante dans leurs groupes d'âges ; en outre ils ont leur propre culture « en ligne », leur propre langage et leur propre « netiquette ». Toutefois, les membres de la génération « née à l'ère du numériquev représentent également un défi considérable car ils manquent d'orientation et ne savent pas toujours ce qu'est un comportement adéquat – concernant le partage des données personnelles ou le partage de contenus sous copyright. Ceci, entre autres, est un fardeau pour eux-mêmes et constitue ainsi une tâche d'éducation pour la société – c'est également un problème tangible pour les modèles économiques numériques, par ex. dans les domaines des contenus numériques ou de la publicité innovante. L'industrie a tout intérêt à parvenir à une vision établie en collaboration afin de déterminer comment aborder la génération née à l'ère du numérique et afin d'établir de nouvelles voies de coopération.

CONCLUSION

Les facteurs identifiés de croissance de l'industrie du numérique entraînent des changements fondamentaux dans tous les domaines de l'économie et de la société. Ce qui est certain, c'est que l'industrie du numérique continuera à mener la croissance et la prospérité économique et qu'elle deviendra un point encore plus central de la vie de tous les jours. L'infrastructure numérique crée de nouvelles voies d'interaction, de communication et de commerce qui se situent encore à leurs débuts et qui attendent d'être pleinement exploitées.

3. FACTEURS PORTEURS DE REVENUS ET DE CROISSANCE : CONTENUS ET PUBLICITÉ, ET NON PAS L'ACCÈS

Les zones de croissance identifiées entraînent une augmentation des revenus dans l'économie numérique à travers quatre catégories de revenus :

La prochaine vague de croissance au sein de l'économie numérique sera alimentée par l'augmentation de la consommation plutôt que par le nombre d'utilisateurs.

1. Publicité – toutes formes de publicité en ligne, y compris les recettes du click-through[1], les publicités IPTV et le sponsoring (par ex. : la télévision en ligne affiche des sponsors « Cette émission vous est présentée par xyz »).

2. Contenus – contenus numériques fournis en ligne, y compris les vidéos à la demande, les jeux, la télévision (la télévision Web payante et le streaming de vidéos) et les téléchargements de musique.

3. E-commerce – produits et services commandés sur Internet et livrés par des moyens traditionnels (par ex. commande de livres sur Amazon ou achat d'un billet d'avion sur le site Web d'une compagnie aérienne).

4. Accès – transport ou trafic vers l'Internet et accès à des offres de télévision numérique, en particulier les recettes perçues par les opérateurs de réseaux (câ-ble et DSL) pour la fourniture de l'accès Internet.

Le e-commerce est la catégorie de revenus la mieux établie et la plus large. La publicité en ligne et les contenus sont des catégories de revenus relativement nouvelles en croissance

(1) Recettes Click-through – recettes réalisées sur la base d'une rémunération du trafic renvoyé depuis un lien sponsorisé sur un moteur de recherche vers un site web.

respectivement de 32 % et 22 %, bien que partant d'un niveau bas. (Voir Illustration 13).

Jusqu'à présent, l'économie numérique a été entraînée dans une large mesure par les avancées technologiques ; la transition des réseaux bas débit vers les réseaux haut débit a créé une explosion dans la pénétration et la consommation Internet. L'accès haut débit est désormais devenu un phénomène de masse dans de nombreux pays européens, asiatiques et américains, ce qui entraîne des degrés élevés de saturation dans certains pays, en particulier en Europe de l'Ouest, avec un retard dans certains pays du Sud et de l'Est de l'Europe. De ce fait, on s'attend à ce que les revenus du marché de l'accès dans ces pays restent stables dans le temps avec un taux de croissance à un chiffre. En même temps, les infrastructures de transport sont de plus en plus standardisées, ceci étant la conséquence d'un marché hautement concurrentiel avec des solutions techniques établies et des opportunités restreintes de différenciation.

Le marché global de l'Internet connaîtra une croissance de 18 % par an pour atteindre un volume de 436 milliards d'€ en 2012.

Le ralentissement de la croissance du nombre de souscripteurs et la croissance modeste des recettes liées au marché de l'accès combinés à la quantité accrue de trafic due à un nombre de plus en plus important d'applications nécessitant une bande passante élevée (par ex. vidéo à la demande, P2P) augmentent la pression sur les marges liées à ce marché. La part de valeur globale associée au marché de l'accès diminuera, passant de 24 % aujourd'hui à moins de 16 % en 2012.

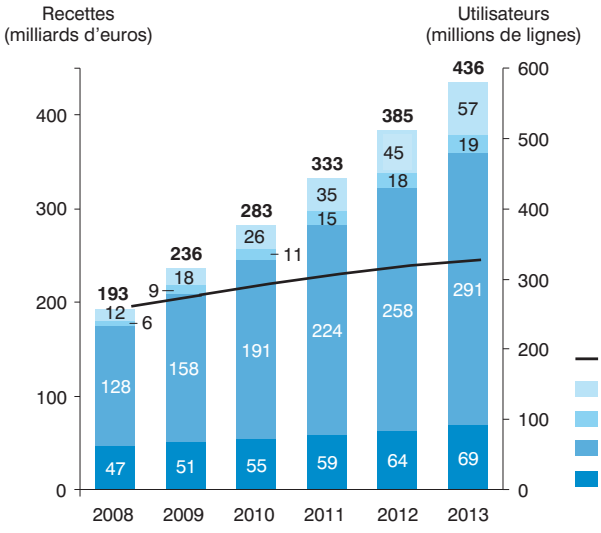
La valeur résidera de moins en moins dans les infrastructures : la part du marché de l'accès Internet diminuera presque de moitié dans les cinq prochaines années – 16 % en 2012 contre 24 % aujourd'hui.

Étant donné que l'on prévoit pour les recettes une croissance plus rapide que celle des utilisateurs d'Internet (taux de croissance composé annuel de 18 % pour les recettes par rapport à 4 % pour les utilisateurs) dans les années à venir, il est évident qu'une modification fondamentale de la répartition des valeurs aura lieu sur la chaîne de valeur. La croissance future proviendra de l'augmentation des recettes générée par la stimulation des dépenses des utilisateurs plutôt que par une augmentation du nombre d'utilisateurs. Il est attendu que cette croissance s'accomplira grâce à des produits et des services plus novateurs, complétés par des nouveaux modèles économiques à même de générer des flux croissants de revenus.

Les opérateurs de réseaux Internet doivent faire face à des niveaux plus élevés de trafic accompagnés d'une diminution des retours.

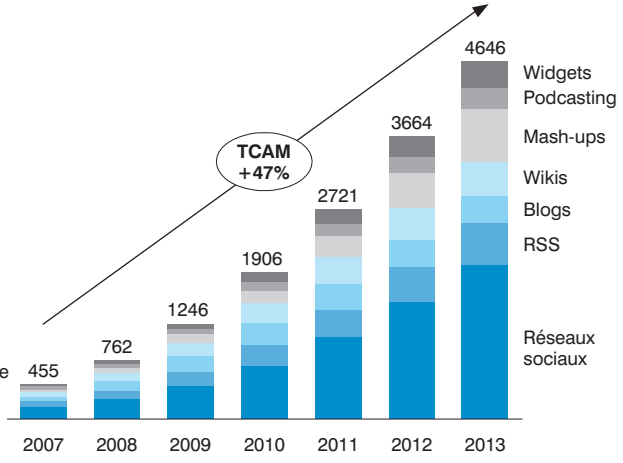
Ces nouveaux services s'appliqueront aussi bien aux consommateurs qu'aux entreprises. Par exemple, Forrester estime que les ventes B2B liées au Web 2.0 connaîtront une croissance de 47 % par an, avec un résultat de presque 5 milliards de $ dans le monde entier avant 2013.

Illustration 13 : Vie numérique—total des revenus en Europe



Note : Europe, comprenant l'UE à 27, la Norvège et la Suisse
Source : Forrester e-Commerce Forecast, rapports d'Apple, rapports de Google, EU TV et modèle prévisionnel haut débit, analyse Booz & Company

Illustration 14 : Chiffre d'affaires mondial annuel « Entreprises 2.0 » (millions de dollars US)

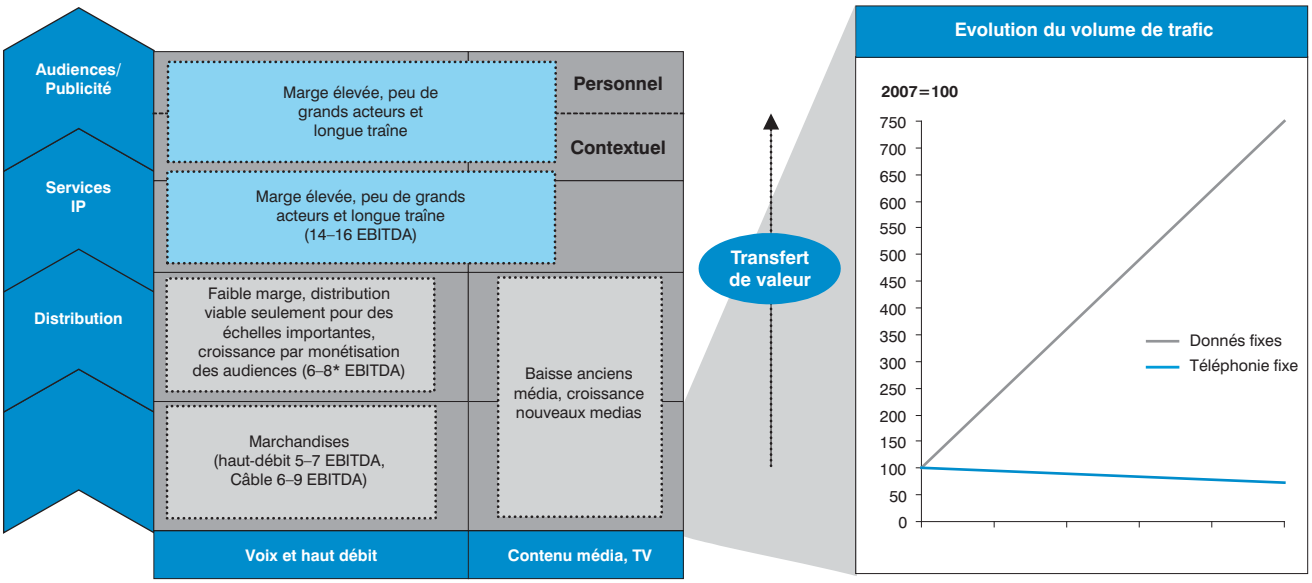


Source : Forrester

Les opérateurs de réseaux doivent adopter de nouveaux modèles économiques générant de la valeur par le biais de services et d'applications plutôt que par l'extension des infrastructures – ils doivent également investir dans des réseaux de nouvelle génération afin de s'emparer de la croissance et d'être en mesure d'offrir des services à valeur ajoutée.

En conséquence, la prochaine vague de croissance de l'économie numérique sera entraînée par les services et applications qui peuvent être uniquement réalisés en parallèle de la pénétration du haut débit par pays. Ainsi, dans ces pays connaissant un clivage considérable sur le plan numérique, l'extension des infrastructures haut débit continue d'être la clé de base de la croissance de l'économie numérique. Dans les pays où les infrastructures haut débit sont plus avancées et proches du point d'inversion sur leur courbe de maturité, les opérateurs de réseaux devront continuer d'inciter à la conversion aux réseaux de nouvelle génération (NGN) afin de se préparer d'une manière générale aux flux de trafic attendus en raison d'un usage accru et notamment de la vaste introduction de la télévision et de la vidéo haute qualité.

Illustration 15: Perspective transport des données



Note : Europe 27+2 (Suisse, Norvège), y compris marchés haut débit moins développés, estimation conservatrice pour marchés développés
Source : Ovum, analyse Booz & Company

III. CONFIANCE NUMÉRIQUE : ASSURER LA CROISSANCE FUTURE DE L'ÉCONOMIE NUMÉRIQUE

1. MENACES POUR L'ÉCONOMIE NUMÉRIQUE

La croissance de l'économie numérique doit être soutenue par une croissance continue de l'usage et des dépenses en ligne. Afin de parvenir à ceci, il est nécessaire que les consommateurs et les entreprises aient confiance en l'environnement dans lequel ils agissent. Les consommateurs devront être éduqués au sujet des menaces potentielles de l'Internet et de la manière de les gérer – et il sera nécessaire qu'ils se sentent en sécurité et qu'ils le soient réellement. Pour l'industrie, l'un des défis principaux sera de fournir un environnement de réseau sécurisé et de procurer une expérience de niveau optimal aux clients.

Le succès de l'industrie du numérique a été accompagné de l'apparition d'inquiétudes de la part des consommateurs et des entreprises en ce qui concerne la sécurité et l'intégrité de l'environnement numérique

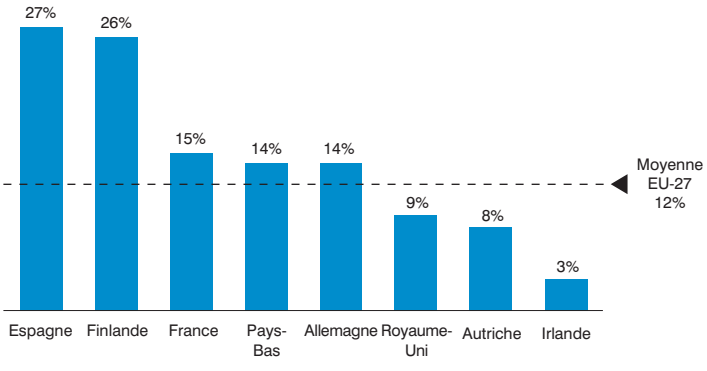
La prolifération des technologies conviviales et d'une connectivité omniprésente a contribué à faire de l'Internet la plateforme principale de l'économie numérique. Les stratégies croisées entre platesformes et la « webification » d'autres platesformes feront également augmenter l'importance et la présence d'autres platesformes telles que la télévision numérique et les platesformes mobiles sur le devant de la scène.

Avec la croissance de l'économie Web 2.0 sont également apparus des motifs d'inquiétude. Premièrement, ceux en lien avec les modèles comportementaux des consommateurs eux-mêmes, par exemple le flux accru d'informations personnelles sur Internet en raison des activités de profilage par le biais des sites de réseaux sociaux. La pression générale exercée sur les fournisseurs de services et de plates-formes pour les inciter à monétiser les applications Web 2.0 (tout particulièrement dans le cas des sites de réseaux sociaux) et les investissements dans les réseaux de nouvelle génération font augmenter la pression commerciale sur les consommateurs, par ex. avec les nouveaux modèles économiques axés sur la publicité, ou d'autres formes de marketing ciblé faisant usage des profils des utilisateurs en ligne. Mais dans la sphère professionnelle également, les profils d'utilisateurs en ligne, les blogs, les albums photo peuvent avoir des conséquences lorsque les futurs employeurs scannent leurs candidats potentiels.

D'autres inquiétudes sont liées aux attaques malveillantes envers la sécurité des réseaux, ceci menaçant la protection des données personnelles en ligne ou la continuité d'exploitation en infirmant la croissance des services dépendants d'environnements de réseaux sécurisés (voir l'Illustration 17). Dans de nombreux cas, ces inquiétudes sont entièrement justifiées ; par exemple, une analyse du palmarès des 10 escroqueries les plus courantes sur Internet aux États-Unis au cours de l'année 2007 a montré que la majorité des cas était liée aux activités de e-commerce, ayant eu pour conséquence des pertes financières réelles et tangibles ayant atteint 4.000 $ (voir l'Illustration 18 pour le palmarès des arnaques Internet les plus courantes). 12 % des Européens évitent de faire du e-shopping en particulier à cause des inquiétudes relatives à la sécurité de l'Internet (voir l'Illustration 16). Outre les activités frauduleuses, les entreprises et sociétés se trouvent menacées par les attaques en nombre croissant d'utilisateurs malveillants ; Data a sous-entendu qu'en 2005 déjà, de telles attaques ont coûté à l'industrie une somme de 1.000

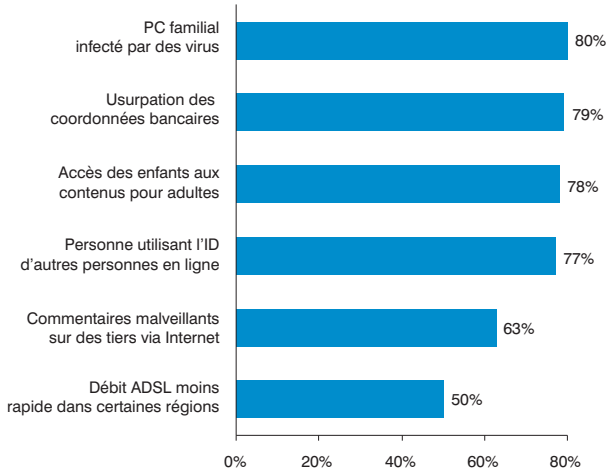
Un consommateur sur huit évite de faire du e-shopping en raison des inquiétudes liées à la sécurité de l'Internet.

Illustration 16 : % de consommateurs évitant les achats sur internet pour des raisons de sécurité (Europe 2007)



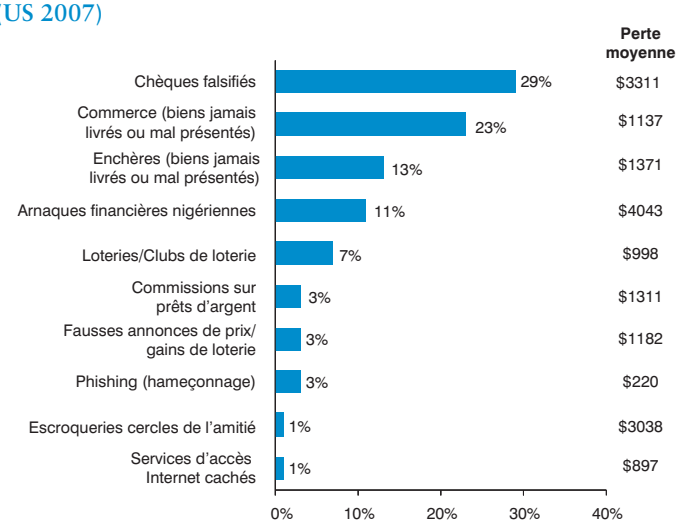
Source : Eurostat

Illustration 17 : Prise de conscience des différents problèmes liés à l'Internet (sondage au Royaume-Uni, 2007)



Source : Ofcom

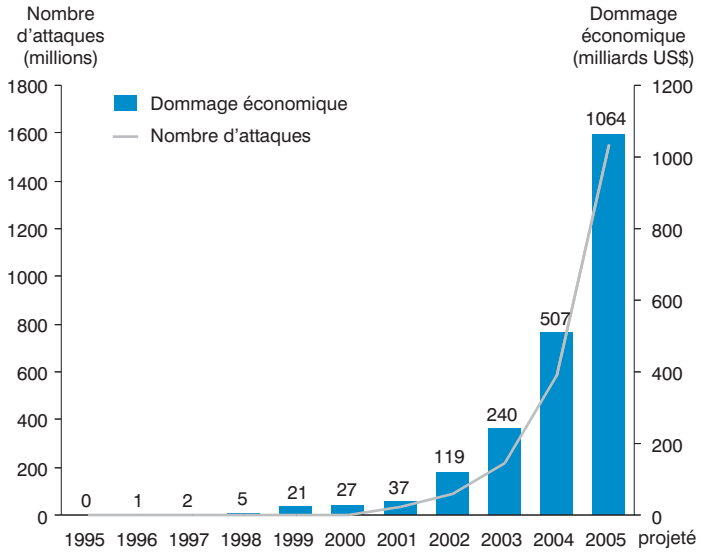
Illustration 18 : Palmarès des arnaques Internet (US 2007)



Source : Centre des fraudes de la NCL

Note pour les ventes aux enchères : en automne 2003, le géant Internet eBay a supprimé le lien vers « fraud.org » de son site web. En conséquence, le nombre de plaintes sur les ventes aux enchères rapporté au Centre des fraudes de la NCL a considérablement diminué.

Illustration 19 : Explosion des attaques numériques avérées (à l'échelle mondiale)



Source : Centre des fraudes de la NCL, mi2g, Craig Fosnock, sondage E-communication des ménages 2007 de Eurobarometer, Symantec, McAfee, analyse de Booz & Company

On entend par attaques avérées :
- les attaques de données visant à violer la confidentialité, l'authenticité ou l'intégrité de données
- les attaques de contrôle visant à compromettre le contrôle du réseau ou de systèmes d'administration

milliards de $ par an dans le monde entier en termes de manque à gagner, de coûts entraînés par le temps perdu, de coûts de réparation des dommages causés aux systèmes et de coûts liés à la perte de réputation. Ces coûts ont augmenté à une rapidité extrême entre 2000 et 2005 en raison de la croissance rapide de l'économie numérique (voir Illustration 19). Aujourd'hui, même les experts de l'industrie ne sont plus en mesure d'évaluer le dommage.

Le Web 2.0 constitue également une force perturbatrice majeure pour l'industrie des contenus audiovisuels en raison de la piraterie en ligne et en raison de l'idée, largement répandue au sein de la génération née à l'ère du numérique, que tous les contenus devraient être gratuits. L'industrie des médias se débat avec la question de l'emploi des standards légaux traditionnels qui obtiennent une acceptation moins forte dans le contexte des activités numériques « ambiguës », par ex. le partage de contenus sous copyright, qui exerce une pression forte sur les industries des médias visant à trouver des méthodes de mise en application efficace de la protection légale dans l'environnement en ligne et d'éducation de la génération née à l'ère du numérique. Le fait d'être « né à l'ère du numérique » n'excuse pas les comportements illégaux mais peut tout au moins en être une explication, étant donné que de tels utilisateurs ont été accoutumés au modèle de l'Internet « gratuit » et qu'ils s'attendent à pouvoir télécharger des contenus numériques sans avoir besoin d'y souscrire ou de les payer.

Pour soutenir la croissance de la vie numérique, il est nécessaire d'éduquer les consommateurs au sujet des menaces et de leur fournir les connaissances et les outils leur permettant de gérer ces menaces.

L'Internet a engendré toute une économie souterraine qui alimente un marché d'activités numériques illégales. Par exemple, il est possible d'acquérir des « produits » numériques tels que des mots de passe et adresses e-mail ou

des services tels que des courriels spam et des « bots » avec des fonctions sur mesure capables de faire des ravages considérables dans les entreprises ciblées. Les entreprises et sociétés reconnaissent ces menaces et commencent à y riposter. Microsoft emploie environ 65 investigateurs et juristes à plein temps pour traquer la cybercriminalité (janvier 2008).

Dans l'ensemble, les risques désormais devenus visibles dans le monde numérique entraînent des inquiétudes de la part des consommateurs et des entreprises, ce qui menace la poursuite de la croissance de l'Internet et de l'économie numérique telle qu'elle a été décrite.

2. CONFIANCE NUMÉRIQUE : CONCEPT ET APERÇU D'ENSEMBLE

Le degré de confiance accordé à l'industrie par les consommateurs traditionnels, comme par ceux nés à l'ère numérique pour la fourniture de services et d'environnements sécurisés, en termes de bonne continuité d'exploitation de même que concernant l'aptitude des gouvernements et des autorités de régulation à protéger les consommateurs, est en train de devenir rapidement un paramètre essentiel en vue de pouvoir assurer la croissance potentielle de la nouvelle économie numérique. De ce fait, la Confiance Numérique est en train de devenir un facteur clé de la croissance – ou un frein à celle-ci – au sein de l'économie numérique, de même qu'elle permet de mesurer à quel point les consommateurs et les fournisseurs de services numériques se fient aux applications numériques au sens le plus large, c.-à-d. à quel point ils se sentent à l'aise en s'engageant dans le numérique.

La Confiance Numérique est un facteur clé de la croissance – ou un frein à celle-ci – au sein de l'économie numérique ; elle permet en outre de mesurer à quel point les consommateurs et les fournisseurs se fient à la vie numérique.

L'industrie a développé une conscience accrue quant à l'importance de démarches proactives dans la Confiance Numérique et a commencé, dans une certaine mesure, à mettre en œuvre de telles démarches. Toutefois, il s'agit ici d'un thème complexe, impliquant de nombreux acteurs qui poursuivent fréquemment des positions et des intérêts divergents, avec des activités entreprises de manière fragmentée et seulement déclenchées lorsque des atteintes à la confiance sont explicitement rapportées.

Pour que l'industrie puisse avancer, il est important de mettre l'accent sur les facteurs clés, sur la base desquels les consommateurs jugeront la performance des entreprises pour ce qui est de fournir de nouveaux services et de nouvelles platesformes numériques et en ligne. Ces facteurs clés sont dérivés d'une analyse des points

Illustration 20 : Les quatre piliers de la Confiance Numérique

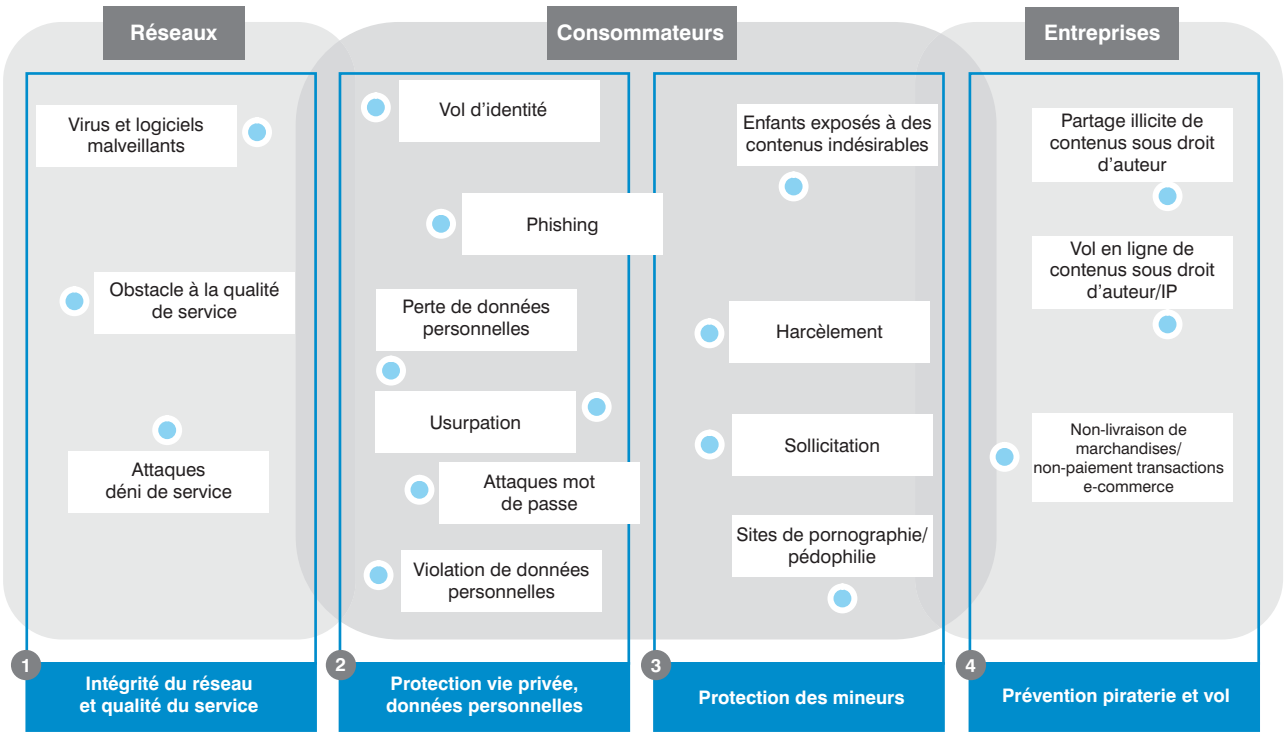
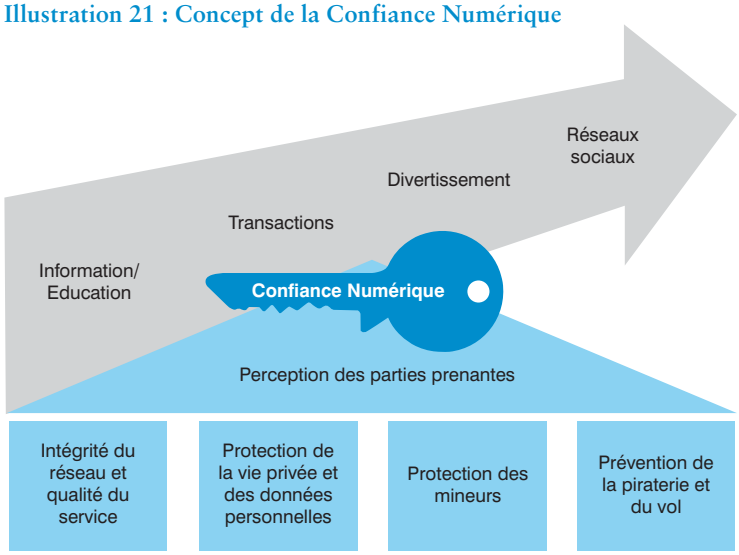


Illustration 21 : Concept de la Confiance Numérique



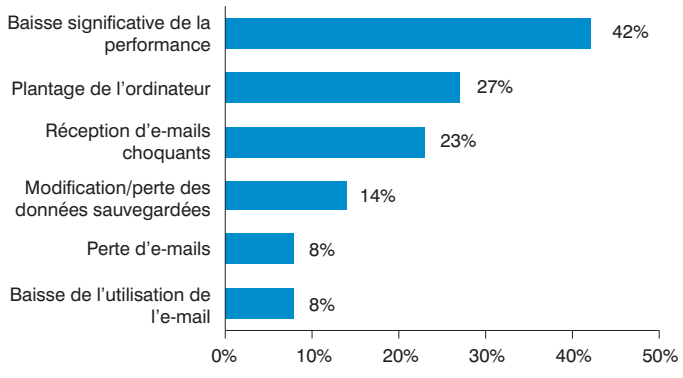
centraux des politiques Web 2.0 actuelles et des processus de légiférération, des débats parlementaires, des accords (de commerce) internationaux, des activités sur les blogs et de l'attention des médias. Ces facteurs se répartissent sur quatre domaines :

- Intégrité du réseau et qualité du service.
- Protection de la vie privée et des données.
- Protection des mineurs.
- Prévention de la piraterie et du vol.

L'industrie a besoin d'agir de manière proactive sur la base d'une vision holistique de toutes ces questions ; c'est cette vision qui a été appliquée, dans le présent rapport, dans le concept de « Confiance Numérique ». Le fait d'encourager la Confiance Numérique dépasse largement la responsabilité et la simple conformité des entreprises – cela devient presque un préalable commercial et l'équivalent d'un permis d'agir. Comme certaines études de cas le montreront, l'observation des prescriptions légales ne permet pas à elle seule d'acheter l'acceptation du consommateur.

**Source : Pew Internet & American Life Project*

Illustration 22 : Problèmes résultant des spams et virus (Royaume-Uni 2007)



Source : Sondage e-communications des ménages 2007 par Eurobarometer

Les quatre piliers sur lesquels s'appuie le concept de Confiance Numérique (voir Illustration 21) englobent les principales menaces, questions et attaques pertinentes aujourd'hui et vécues en tant que telles par les consommateurs. Ce cadre structure et identifie les risques devant être abordés ainsi que les objectifs de la Confiance Numérique pour chaque pilier :

- **Intégrité du réseau et qualité du service :** comment maintenir l'intégrité du réseau face aux attaques informatiques malveillantes ? Comment mettre en place des pratiques de gestion des réseaux à même d'optimiser l'expérience faite par le client ? Assurer une répartition équitable de la bande passante du réseau pendant les heures de pointe, gérer la croissance du trafic, protéger contre les logiciels malveillants.

- **Protection de la vie privée et des données :** comment manier et protéger les données et la vie privée des consommateurs en ligne ? Prévenir le vol d'identité, la perte accessoire de données privées et l'exploitation commerciale des données.

- **Protection des mineurs :** comment garantir la sécurité des enfants en ligne ? Protéger ceux-ci contre les contenus indésirables, contre le harcèlement et le grooming, et lutter contre les contenus de pornographie enfantine.

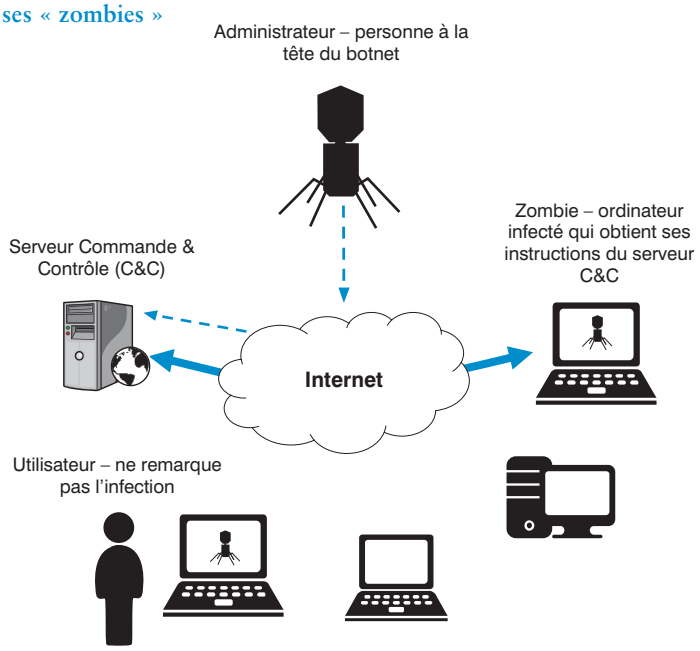
- **Prévention de la piraterie et du vol :** comment gérer les violations de copyrights ? Contrer le vol de contenus sous copyright, protéger les transactions de e commerce.

À travers ces quatre piliers, tout un ensemble de parties prenantes influe sur le degré de Confiance Numérique ou, au contraire, est affecté par celui-ci.

Le présent rapport a pour but de mettre l'accent sur certaines études de cas relatives aux meilleures pratiques de la Confiance Numérique et de révéler ce qui est nécessaire pour accélérer les initiatives proactives devant être déployées et

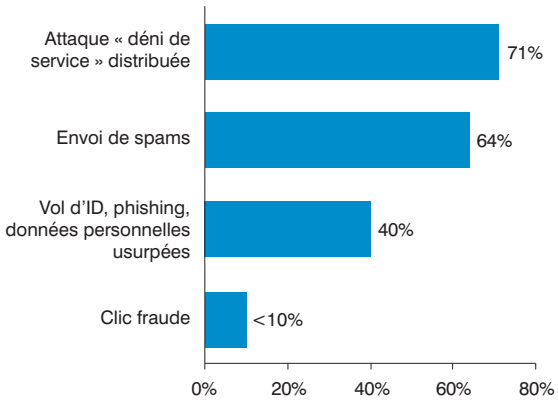
*Les réseaux sociaux facilitent le harcèlement en ligne – on observe une augmentation de 70 % du harcèlement subi par les mineurs utilisant des réseaux sociaux.**

Illustration 23 : Réseaux botnets—l'administrateur de robots et ses « zombies »



Source : WatchGuard

Illustration 24 : Utilisation des botnets pour attaques



Source : Arbor

menées par l'industrie. Il a pour but de contribuer à la réflexion concernant les « niveaux d'intervention » appropriés et proportionnellement adéquats et les formes de coopération entre industrie et gouvernements – pour encourager la Confiance Numérique dans l'alignement des libertés fondamentales sur Internet comme des exigences économiques.

3. ASSURER L'INTÉGRITÉ DU RÉSEAU ET LA QUALITÉ DU SERVICE

Le pilier « Intégrité du réseau et qualité du service » met l'accent sur la protection des plates-formes technologiques permettant l'économie numérique. Il a deux objectifs essentiels :

1. Garantir que la plateforme de réseau et l'environnement informatique sont sécurisés pour les consommateurs et les entreprises et protégés des attaques externes – contrer les perturbations infligées aux consommateurs et aux entreprises par les attaques numériques malveillantes, par exemple les virus, les logiciels malveillants tels que les logiciels espions et les chevaux de Troie qui collectent ou détruisent les informations, et la submersion ou le spamming de sites Web entraînant un déni de service.[2]

Le spamming fait baisser la confiance des consommateurs dans les e-mails, et 18 % le considèrent comme un gros problème.

2. Garantir que les utilisateurs finaux bénéficient d'une qualité de service régulière et constante – garantir que le réseau soit capable de gérer les volumes croissants de trafic tout en assurant aux utilisateurs finaux la qualité du service en dépit des heures de pointe et des surcharges du trafic qui soumettent les ressources du réseau à des contraintes plus élevées

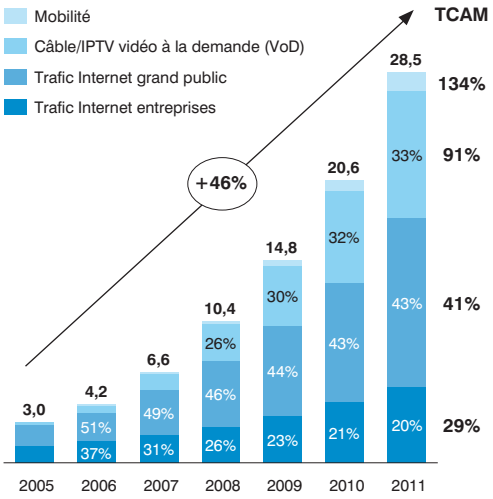
VIRUS ET LOGICIELS MALVEILLANTS

Les virus et les logiciels malveillants sont des attaques délictueuses envers les équipements des utilisateurs finaux et les réseaux localisés qui débouchent sur divers problèmes (voir Illustration 22). Le degré de prise de conscience concernant les problèmes de spamming et de virus varie considérablement en fonction du niveau d'usage de l'Internet. Les pays ayant un niveau élevé d'usage de l'Internet évaluent et comprennent mieux le risque de telles attaques et les degrés de sécurité employés. Par exemple, les pays nordiques et le Benelux ont une conscience élevée des attaques numériques malveillantes : plus de 35 % pensent avoir déjà eu des problèmes de spamming et de virus. Par contre, la prise de conscience de tels risques est relativement faible en Europe du Sud – moins de 15 % pensent avoir déjà eu de tels problèmes. Aux États-Unis, 55 % des usagers d'Internet déclarent que le spamming a fait baisser leur confiance dans les e-mails, et 18 % considèrent le spamming comme un « gros problème ».

Les botnets sont responsables de 80 % du spamming dans le monde entier.

(2) Lors d'une attaque « déni de service » (DdS), un grand nombre d'ordinateurs envoie du trafic à un seul ordinateur cible, provoquant une surcharge extrême de la cible avec des données et monopolisant ainsi toutes les ressources. En conséquence de ceci, le système cible s'effondre ou devient pour le moins inutilisable.

Illustration 25 : Croissance globale du trafic IP (2005–2011, en exaoctets par mois)



Source : Cisco

Les conséquences les plus fréquentes du spamming, des virus et des logiciels espions sont habituellement d'endommager l'équipement informatique. L'Union des Consommateurs a découvert que sur une période de six mois, les infections par des logiciels espions ont obligé presque un million de ménages aux États-Unis à remplacer leur ordinateur.

Étant donné que le degré de prise de conscience des consommateurs augmente à l'égard de ce risque particulier, il apparaît que ceux-ci sont de plus en plus disposés à assumer une certaine responsabilité dans la prévention des virus et du spamming affectant leur équipement informatique. En effet, le commerce global des logiciels de sécurité a aujourd'hui une valeur de 9,1 milliards de $ par an et un taux de croissance d'environ 12 % par an.

(3) Les bots sont des logiciels installés sur un système local et recevant des ordres d'un serveur de contrôle à distance. Le bot exécute la tâche de manière aussi autonome que possible et attend ensuite de nouveaux ordres.

Éducation des mineurs et intégrité du réseau

France, mai 2008 : les autorités arrêtent 22 personnes suspectées d'être des pirates informatiques agissant au sein d'un réseau international de piraterie. Fait perturbant après les arrestations : 16 suspects parmi les 22 ont moins de 18 ans.

Les experts en sécurité de Sophos applaudissent le succès des autorités, mais ils s'interrogent : « Qu'est-ce qui ne fonctionne pas dans notre éducation de la population jeune et qui leur fait penser que la piraterie informatique pourrait être un comportement acceptable ? » « Il est nécessaire d'agir plus pour enseigner aux enfants à l'école comment utiliser de manière responsable leurs compétences à l'ordinateur. »

BOTS, ZOMBIES ET BOTNETS

Un bot est un logiciel utilisé pour automatiser des tâches spécifiques de manière semi-intelligente.[3] Les bots peuvent être utilisés de manière nocive par un attaquant (le bot herder) pour contrôler à distance d'autres ordinateurs appelés des ordinateurs zombies, tel que ceci est représenté sur l'Illustration 23. L'attaquant peut ensuite accomplir quasiment toutes les tâches qu'il souhaite sur l'ordinateur zombie.

Les botnets sont utilisés dans plusieurs buts, par exemple pour le spamming et les attaques déni de service, pour le phishing (hameçonnage) ou encore pour la clic-fraude (La clic-fraude est une attaque contre les fournisseurs de publicité ; le bot fait semblant de cliquer sur des annonces plusieurs milliers de fois par heure) et pour le vol d'identité (voir Illustration 24).

La bande passante combinée de plusieurs milliers d'ordinateurs - pour la plupart équipés de connexions haut débit - peut provoquer des attaques déni de service (DdS) considérables et estimées responsables de 80 % du spamming dans le monde.

Un botnet met tous les zombies sous le contrôle d'un seul bot herder. Quelques botnets célèbres :

- **Kraken :** presque 500.000 zombies, y compris les ordinateurs infectés dans 50 entreprises Fortune-500 ; quasiment indétectable par les logiciels anti-virus
- **Srizbi :** plus de 300.000 zombies
- **Storm :** environ 150.000 à 200.000 zombies
- **Bobax :** éventuellement un prédécesseur de Kraken ou un botnet distinct

Il n'y a pas que les consommateurs et les entreprises qui soient victimes de botnets. Même des pays peuvent en être la cible, comme le montre l'attaque déni de service par des botnets contre l'Estonie en 2007. Les cibles des attaques déni de service comprenaient le parlement présidentiel estonien, presque tous les ministères du gouvernement estonien, les partis politiques, trois parmi les six grandes institutions d'information du pays, deux des plus grandes banques et des sociétés spécialisées dans la communication.

QUALITÉ DU SERVICE

Dans la mesure où les problèmes de qualité du service reposent sur le réseau (la qualité du service dépend de la trajectoire parcourue d'un bout à l'autre de l'Internet, et non pas uniquement du

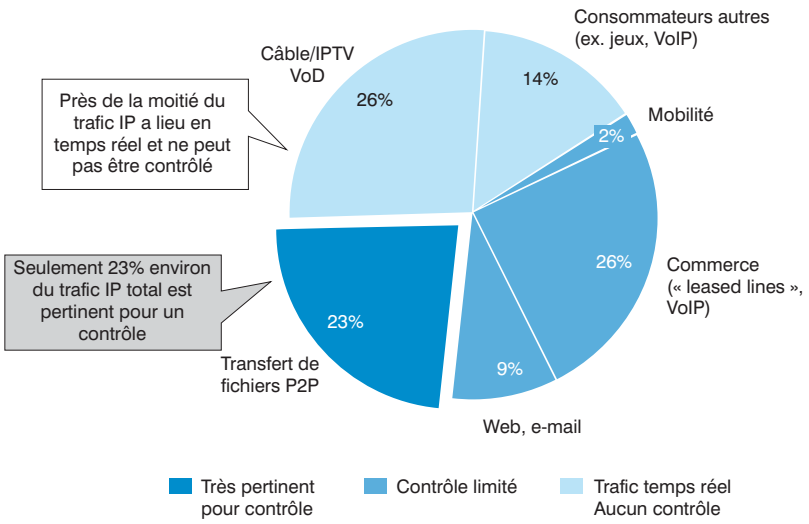
réseau d'accès), ils résultent de deux facteurs principaux : le volume croissant du trafic Internet en général et les pointes de trafic en raison des usagers lourds utilisant simultanément des applications exigeant une bande passante importante. Le volume du trafic Internet a connu une croissance particulièrement rapide au cours des dernières années - et il est également prévu que cette croissance soit maintenue dans le futur (Illustration 25). De ce fait, il est nécessaire de prendre des mesures visant à gérer les augmentations de trafic résultant d'applications telles que la vidéo à la demande, la HDTV, le partage de fichiers, la vidéo générée par les utilisateurs, les contenus de grande taille, le P2P et les jeux en ligne – toutes ces applications étant appelées à porter la nouvelle vague de croissance dans l'économie numérique. La QdS (qualité du service) dans le présent rapport concerne uniquement les services IP – les opérateurs de réseaux assurent la QdS dans les services vidéo basés sur DVB-C en utilisant un spectre consacré qui n'a aucun impact sur les vitesses Internet haut débit. Ceci est différent dans un environnement IP où des flux IPTV (multiples) imposent une contrainte pesant sur la capacité haut débit.

Le deuxième point d'inquiétude concerne les « utilisateurs lourds ». Les réseaux haut débit – comme tous les réseaux – sont conçus pour répondre aux pointes et aux surcharges prévues qui surviennent pendant les périodes d'occupation maximale des réseaux. Les utilisateurs lourds entraînent des pointes du volume du trafic qui excèdent les charges maximales prévues lors de la conception. Sans une gestion active du réseau, les utilisateurs finaux connaîtraient une dégradation de la qualité du service reçu – bien que le degré de cette dégradation puisse varier en fonction de l'application (par ex. la banque en ligne par rapport aux téléchargements mp3). Dans les réseaux haut débit où la capacité est une ressource partagée, cet effet se manifesterait par une vitesse de connexion réduite ou, dans les cas extrêmes, par une interruption du service.

Les utilisateurs lourds imposent des contraintes pesant sur la qualité du service pour tous les usagers

Afin de contrer les effets impliqués par des volumes de trafic dépassant les capacités du réseau, les opérateurs pourraient ajouter des capacités supplémentaires (en construisant de nouvelles infrastructures et en actualisant celles qui existent) en engageant des dépenses d'investissement et des coûts fixes, ou en mettant en application des techniques de gestion active du trafic afin de sauvegarder la bande passante pour des types spécifiques de trafic en faveur de tous les usagers.

Illustration 26 : Contrôle du trafic, applicabilité—répartition du trafic IP global 2008



Source : Cisco, analyse Booz & Company

Du point de vue de la capacité elle-même, l'ajout de capacités supplémentaires semble être une option évidente, mais elle a également un impact économique considérable. En raison de la rapidité de croissance du trafic, les fournisseurs de réseaux seraient contraints d'ajouter de plus en plus de capacités, ce qui entraînerait également une augmentation croissante des coûts de mise à jour des réseaux. Sur la base du modèle économique du fournisseur de réseau, ces coûts doivent être portés par les consommateurs utilisant le réseau – ceci provoquant ainsi des augmentations des prix à payer par les utilisateurs finaux. De plus, une capacité accrue ne résoudra pas à elle seule la question de la congestion du réseau ni celle de la dégradation du service aux heures de pointe. En fonction du type d'application Internet, de la dimension du réseau ou de la vitesse de l'équipement source, il se pourrait bien que le pic de trafic utilise toujours le maximum de la bande passante disponible, indépendamment de toutes les actualisations de capacité pouvant être réalisées par le fournisseur de réseau.

Pour atténuer la congestion provoquée par l'usage lourd que génèrent les applications 'fortes consommatrices de bande passante, les opérateurs de réseaux déploient des techniques de gestion active du trafic. Outre les solutions techniques de gestion du trafic, des modèles de prix basés sur l'usage sont également pris en considération. Les modèles basés sur les prix encouragent les utilisateurs à éviter les heures de pointe dans leur utilisation de l'Internet et les poussent à se mettre en ligne à d'autres moments.

La gestion technique active du trafic est fréquemment évoquée comme une gestion de la bande passante ou un contrôle du trafic. Ces mesures

techniques détectent le trafic non prioritaire et ne nécessitant pas un traitement immédiat, et lui donne un ordre de priorité plus faible sur le réseau. En conséquence de cette gestion de la bande passante, les téléchargements de données en temps différé, par ex. le téléchargement de musique sur iTunes, prendrait un peu plus de temps – cependant, l'usage d'applications en temps réel, par ex. la transmission de musique en continu ou la téléphonie VoIP, pourrait continuer sans être touché par une telle gestion active.

Néanmoins, la gestion du trafic ne peut qu'être une partie seulement de la solution visant à assurer un flux optimal du trafic sur les réseaux haut débit. Une gestion du trafic basée sur le contrôle sans impact significatif sur les utilisateurs finaux peut être uniquement appliquée sur le trafic en temps différé, ce qui représente entre un quart et la moitié seulement du trafic réel IP, tel qu'indiqué sur l'Illustration 26.

Depuis un certain temps, l'industrie a reconnu qu'une faible proportion d'usagers est responsable d'une part disproportionnée du trafic sur le réseau. Pour de nombreux fournisseurs de réseau, environ 80 % de la bande passante sont consommés par moins de 10 % des usagers. Cela représente non seulement une disparité en termes d'équité dans l'usage, mais cela exacerbe en outre le problème de la bande passante pendant les périodes de pointe. Cet usage lourd est fréquemment en relation avec les applications pair-à-pair et vidéo, et les opérateurs de réseau sont particulièrement préoccupés par la congestion due à ces deux applications très populaires. Un exemple d'augmentation soudaine de la bande passante en raison du streaming de vidéos a notamment été l'introduction du iPlayer par la BBC.

Moins de 10 % des usagers sont responsables de plus de 80 % du trafic du réseau.

La situation au Royaume-Uni liée à la plateforme iPlayer de la BBC est typique du dilemme auquel l'industrie doit faire face. Le iPlayer est utilisé pour distribuer et lire des contenus vidéo et radio sur Internet. Plus de 42 millions de programmes ont été transmis en continu ou téléchargés au cours des trois premiers mois de service ayant suivi le lancement officiel en décembre 2007. Ceci a provoqué de vifs débats au Royaume-Uni entre l'opérateur de la plateforme, la BBC, plusieurs fournisseurs d'accès Internet et les organes de régulation, en raison du niveau d'usage sans précédent et du trafic généré par la plateforme. De nombreux FAI concernés par les exigences de bande passante ont demandé à la BBC une participation au financement des mises à jour nécessaires du réseau. La BBC a rejeté ces demandes jugées « provocatrices », mettant en garde les FAI qu'au cas où les fournisseurs de contenus surprendraient certains opérateurs en train de « restreindre, contrôler ou plafonner » leurs contenus, ils indiqueraient alors sur leurs sites avec quels FAI leurs contenus fonctionnent au mieux – et lesquels il convient d'éviter.

OFCOM a évalué que subvenir au trafic additionnel de 3 GO/mois généré par utilisateur par le iPlayer coûterait aux fournisseurs de réseau du Royaume-Uni jusqu'à 831 millions de £ sur cinq ans pour la mise à jour des capacités de leurs réseaux. Pour les FAI, la question est de savoir qui devra finalement payer les besoins supplémentaires de capacité – le fournisseur de la plate-forme ou le consommateur. En réponse à ces préoccupations, OFCOM a, en avril 2008, confirmé sa position en déclarant que « le poids des investissements [doit] être assumé par les opérateurs de réseaux et les consommateurs, avec des prix susceptibles d'augmenter pour les connexions plus rapides. » (Ed Richards, directeur général d'OFCOM). OFCOM argumente en faveur de « modèles de tarif axés sur les contenus » là où les FAI et les fournisseurs de contenus établissent conjointement des services garantis bien fonctionner sur le réseau, bien que situés à des niveaux de prix appropriés pour le consommateur.

La gestion du trafic et des capacités du réseau a des avantages clairs pour la majorité des utilisateurs finaux, garantissant à ceux-ci la continuité de la qualité de service qu'ils attendent. Cependant, étant donné que le trafic continue d'augmenter du fait des applications exigeant une grande bande passante telles que la vidéo à la demande, les investissements supplémentaires devront être soutenus par des prix plus élevés, des accès sous forme de produits plus échelonnés ou des méthodes clairement différenciées de gestion du trafic aux périodes de pointe. Par définition, les techniques de gestion du trafic tentent d'établir un équilibre dans les compromis entre la qualité du service, les dépenses d'investissement dues à l'extension du réseau tout en parant à l'augmentation des prix à payer par les utilisateurs finaux pour couvrir les coûts.

La gestion des pointes de trafic est une manière efficace d'assurer la qualité du service pour une vaste majorité d'utilisateurs.

La transition des réseaux haut débit actuels vers des réseaux de nouvelle génération possédant des capacités considérablement supérieures aidera, d'une certaine manière, à pourvoir aux demandes accrues de haut débit associées aux services et applications en temps réel. Ceci ne signifie cependant pas que la gestion du trafic perdra toute signification pour les services gérés en différés.

Étude de cas BBC iPlayer

Conformément aux données fournies par le FAI britannique Plusnet en février 2008, le trafic a connu des pointes considérables depuis le lancement du iPlayer :

- Le streaming de vidéos par utilisateur est passée de 180 MO en décembre à 292 MO en janvier, soit une augmentation de 62 %.
- Les diffusions en streaming dépassent les téléchargements selon un rapport de 8 à 1.
- Le coût du trafic lié au streaming a triplé dans le même temp.

Les faits évoqués ci-dessus pourraient indiquer une tendance selon laquelle les utilisateurs, lorsqu'ils ont le choix entre une option de streaming de bonne qualité et la possibilité du téléchargement, préfèrent le streaming plutôt qu'attendre un téléchargement complet. Il existe probablement une différence dans la manière dont les usagers consomment la musique et la vidéo ; ils peuvent préférer posséder la musique grâce à un téléchargement tout en étant satisfaits de visualiser une vidéo par le biais d'une lecture en streaming.

Si cela s'avérait une réelle tendance, alors la gestion active du trafic sera d'autant moins efficace qu'elle ne s'appliquera pas à des flux à gérer en temps réel. La nécessité d'augmenter les capacités en deviendrait encore plus importante.

APERÇU D'ENSEMBLE DE LA GESTION ACTIVE DE TRAFIC

Il existe divers mécanismes techniques permettant aux opérateurs de réseaux une gestion active du trafic sur leur propre réseau et une optimisation de la bande passante disponible. Tous visent pour l'essentiel à sauvegarder la bande passante consommée par des flux de trafic spécifiques pendant les périodes de pointe et en cas d'usage lourd. Les méthodes se basent sur deux éléments : (I) identification du trafic devant être contrôlé ; (II) réduction de la priorité de ce trafic, et donc réduction de la bande passante utilisée par les trafics sélectionnés.

IDENTIFICATION ET SÉLECTION DU TRAFIC

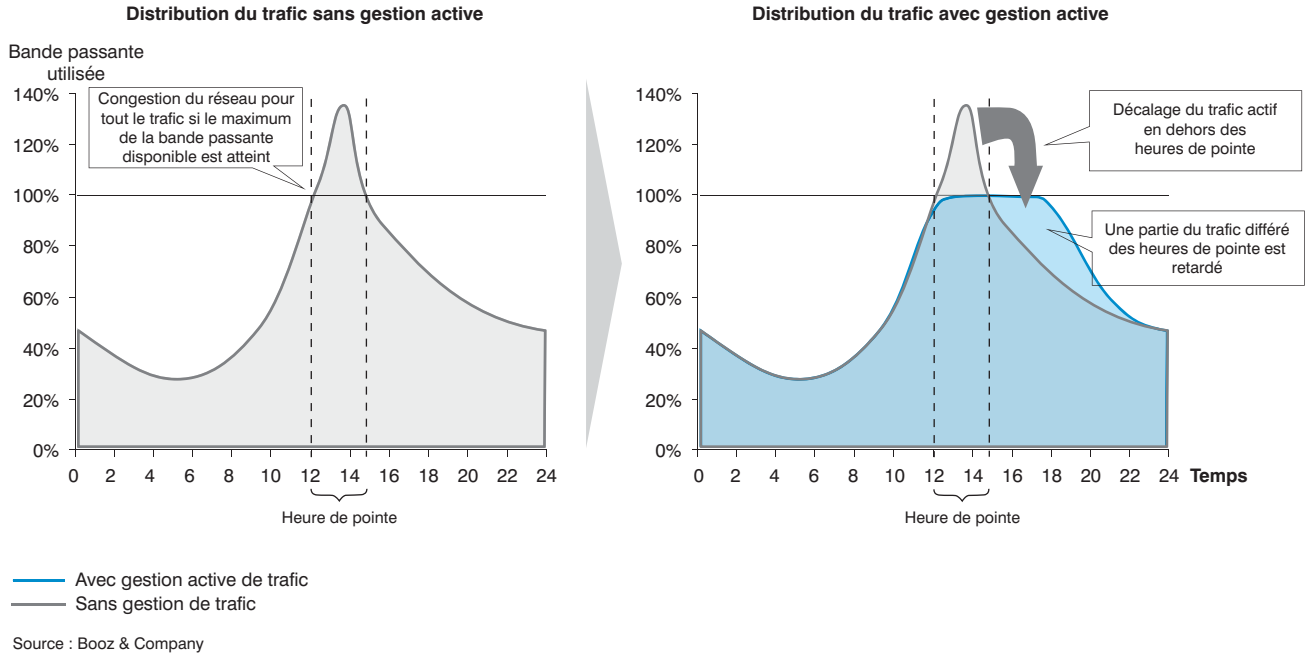
L'identification du trafic apte à un contrôle peut avoir lieu de différentes manières, voir pour cela l'Illustration 28. Une manière simple se base seulement sur les adresses et les ports IP sources ou cibles (par ex. pour faire respecter des limites de bande passante dans le but d'un usage équitable). L'identification du trafic sur la base des adresses et ports IP n'est pas bien ciblée étant donné qu'elle sélectionne des tronçons très larges du trafic qui peuvent toucher de multiples applications (par ex. si un port est utilisé par plusieurs systèmes).

En alternative, une méthode plus sophistiquée d'identification du trafic pour le contrôle est la large vérification de paquets (DPI). Chaque paquet IP est profilé, de telle sorte que le protocole sous-jacent peut être lu et qu'une signature peut être produite. Cette signature peut être comparée à une liste de signatures connues afin de classifier le paquet, par ex. comme étant une vidéo à la demande. Sur la base de cette identification, des protocoles voire des services spécifiques peuvent être sélectionnés ou désélectionnés (dans le cas d'applications en temps réel) pour le contrôle. Un aspect crucial de la DPI est la nécessité de maintenir et d'actualiser fréquemment les bases de données contenant les signatures afin de faire face à l'évolution rapide de l'architecture Internet.

Le plus grand inconvénient de la DPI est son coût : étant donné que chaque paquet doit être individuellement vérifié, un équipement important est nécessaire. Les systèmes utilisent habituellement une méthode hybride par laquelle le trafic est pré-filtré, sur la base de l'adresse et du port IP, et la DPI est uniquement appliquée aux paquets sélectionnés.

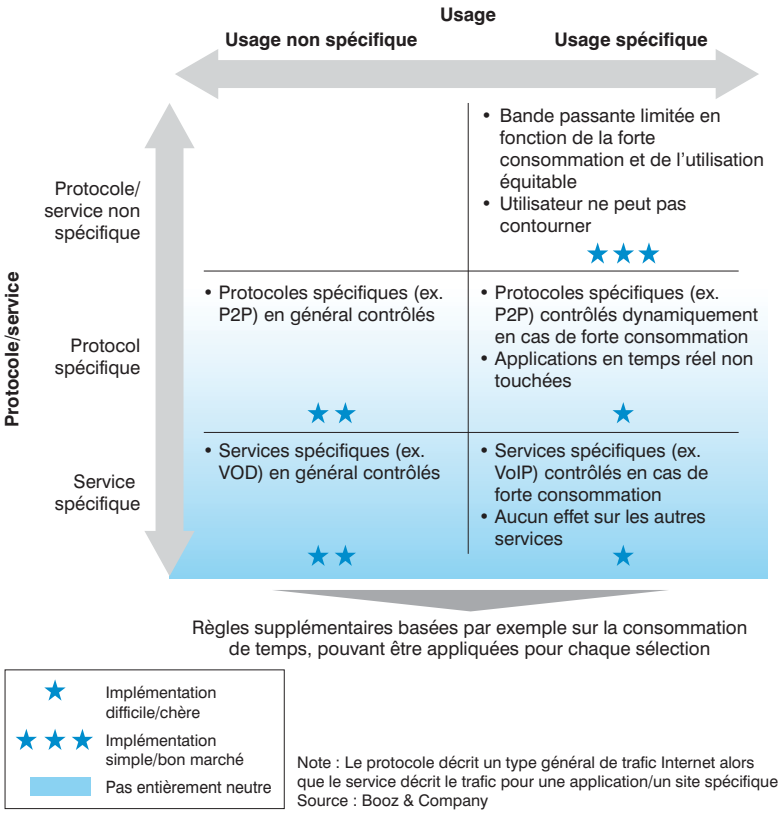
En résumé, la sélection du trafic peut être spécifique à l'utilisateur (sur la base des adresses IP), spécifique au protocole (sur la base de la sélection de port ou de la DPI, par ex. protocole

Illustration 27 : Aperçu d'ensemble—gestion du trafic



Source : Booz & Company

Illustration 28 : Outils de contrôle de la bande passante—quels mécanismes ?



Note : Le protocole décrit un type général de trafic Internet alors que le service décrit le trafic pour une application/un site spécifique
Source : Booz & Company

de mail) et/ou spécifique au service (lorsque le service est un certain serveur ou une application, par ex. YouTube ou BitTorrent).

DÉFINITION D'UN ORDRE DE PRIORITÉ DU TRAFIC

Il existe plusieurs méthodes permettant d'augmenter ou de réduire la priorité et donc la bande passante consommée par des flux de trafic spécifiques. Certaines de ces méthodes peuvent être utilisées dans chaque réseau IP, tandis que d'autres sont spécifiquement conçues pour certains réseaux. Par exemple, PCMM (packet cable multi media) est une solution QdS spécifiquement créée pour les réseaux câblés.

Toutes les techniques reposent sur un ralentissement du trafic sélectionné et réduisent ainsi le flux de données sur le réseau. Du point de vue de l'utilisateur final, l'application d'une gestion de trafic sur le trafic géré en différé ralentira uniquement les téléchargements d'une longue durée sans avoir aucun impact sur les e-mails ou la navigation.

4. PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

La protection de la vie privée et des données concerne les inquiétudes des individus relatives à la sécurité de leurs données numériques personnelles. Elle a quatre objectifs principaux :

1. Protéger les données privées des consommateurs contre la publication – celle-ci pouvant être réalisée par inadvertance ou délibérément (par ex. sur des sites Web de réseaux sociaux), par piratage des bases de données des opérateurs ou par transfert imprudent ou insécurisé de données.

2. Prévenir l'utilisation commerciale des données privées des consommateurs, par ex. comme soutien de nouveaux modèles économiques basés sur la publicité sans que les individus en soient avertis. Par exemple : entreprises utilisant les informations relatives au statut conjugal et à la situation de famille à des fins de publicité en ligne personnalisée et ciblée.

3. Protéger les données privées des consommateurs contre les accès illégaux – par exemple par des moyens tels que la falsification et le phishing.

4. Prévenir le vol d'identité et la fraude – c'est-à-dire lorsque des criminels se procurent de l'argent ou d'autres avantages en reproduisant et en utilisant les données numériques privées de quelqu'un d'autre.

La protection de la vie privée et des données se concentre essentiellement sur deux situations : premièrement, la publication par inadvertance ou délibérée et deuxièmement, les données obtenues illégalement par l'intermédiaire de méthodes telles que le phishing.

*Chaque personne a en moyenne 36 GO de données enregistrées auprès d'institutions – l'équivalent de 80 heures de vidéo ou d'1 million de pages de texte.**

PUBLICATION DE DONNÉES

Sur Internet se développe une véritable prolifération des sites Web de réseaux sociaux, que ce soit ceux ayant des centres d'intérêts généraux (par ex. Facebook) ou ceux qui mettent plus l'accent sur la mise en réseau professionnelle (par ex. LinkedIn). Ces sites Web recueillent, stockent et publient des quantités croissantes d'information sur les usagers, y compris : le lieu de résidence, l'âge, les centres d'intérêt et des photographies. La majorité des sites Web donnent la possibilité de limiter les utilisateurs pouvant consulter les informations du profil détaillé – presque la moitié des utilisateurs rendent cependant leur profil accessible à chacun. De même, de nombreux autres sites Web exigent l'inscription de l'utilisateur pour pouvoir être utilisés (par ex. les fournisseurs de messagerie internet) ou pour accéder à l'ensemble des fonctions et contenus (par ex. de nombreux systèmes de forum) – ces sites collectent également les données des usagers et de leur comportement lorsqu'ils sont utilisés.

Le fait de rendre de telles informations accessibles au public a des conséquences sur la sécurité personnelle et sur la réputation individuelle – par exemple la menace du vol d'identité, ou encore lorsque des entreprises ou sociétés utilisent des informations personnelles sur des sites Web sociaux pour contrôler la validité des informations contenues dans une candidature pour un poste ou pour vérifier l'adéquation d'un candidat à un poste en se basant sur des recherches de communautés professionnelles. De plus, une information ayant été diffusée un jour dans le monde numérique sur Internet ne pourra plus en être « retirée » étant donné qu'il est extrêmement facile de copier, de distribuer et de sauvegarder des données.

*Les usagers d'Internet sont de plus en plus conscients de leur empreinte numérique – 47 % effectuent des recherches d'information en ligne sur eux-mêmes. Mais 60 % ne sont pas inquiets de savoir combien d'informations peuvent être trouvées en ligne.***

Au-delà des consommateurs eux-mêmes, les entreprises et sociétés sont également une source de risque pour la vie privée et les données. De par leur nature même, les informations stockées numériquement sont plus pratiques à gérer, à traiter et à partager pour les organisations. En même temps, le risque qu'elles soient rendues accessibles au public par inadvertance est plus grand, tel que l'a montré un cas récent au Royaume-Uni. Le HMRC, l'organisme public britannique chargé de la collection de l'impôt et des douanes, a été contraint de s'excuser auprès des clients de la banque d'investissement UBS Laing & Cruickshank suite à la perte d'informations sensibles sur les comptes. Le HMRC avait en effet perdu un disque informatique envoyé par la banque et contenant les adresses et les détails des comptes des investisseurs du Personal Equity Plan d'UBS. Cet événement a été causé par une erreur personnelle – il illustre cependant à quel point le risque est réel et considérable.

*La CIA américaine utilise Facebook pour recruter de nouveaux employés.****

Les entreprises et sociétés tirent également profit des informations détaillées dont elles disposent sur leurs clients comme soutien pour leurs opérations commerciales régulières.

**Source : IDC*

***Source: Pew Internet & American Life Project*

****Source: Wired, 2007*

Second Life – Le danger de finir au mauvais endroit

En 2008 en Allemagne, une mère rapporta que sa fille de 13 ans avait commencé à s'impliquer dans Second Life – une plateforme virtuelle qui permet aux utilisateurs de prendre une « identité virtuelle » et de « vivre » dans un monde virtuel.

La fille demanda un jour à sa mère de l'argent pour acheter des Linden Dollars, la monnaie utilisée dans Second Life. La mère refusa de financer ces activités.

Plusieurs mois après, elle découvrit que sa fille avait commencé à se produire comme strip-teaseuse virtuelle, puis qu'elle se vendit comme prostituée virtuelle dans un « club » de Second Life à l'environnement sexuel très explicite afin de gagner des Linden Dollars.

Par exemple, un « Super Serveur » tel que Meredith, une société de médias des États-Unis, vend des extraits de sa base de données contenant des informations sur 85 millions de citoyens des États-Unis et comprenant des détails sur 6 femmes sur 10 et sur 8 ménages sur 10. Elle a incorporé dans ses opérations des agences de publicité numérique afin de monétiser la valeur des informations qu'elle détient par le biais de la publicité ciblée.

Missouri/USA, mai 2008 : le harcèlement en ligne devient illégal suite à un suicide

Suite au suicide d'une jeune fille de 13 ans harcelée en ligne par des voisins, une législation est envisagée pour rendre illégal le harcèlement en ligne. La persécution et l'intimidation sont sanctionnées par des peines allant jusqu'à deux ans d'emprisonnement.

Les premières réactions font part de la difficulté de déterminer une « persécution » en comparaison avec l'interaction « normale » ou la plaisanterie entre amis. De plus, la mise en application de la loi est considérée d'un œil critique.

PHISHING

Le phishing est la méthode la plus courante visant à obtenir illicitement les données privées d'individus. Il implique le « déguisement » en une entité digne de confiance afin d'obtenir des informations sensibles telles que les noms d'utilisateur, les mots de passe et les détails de cartes de crédit. Les cibles des attaques de phishing sont les utilisateurs finaux, la majorité (plus de 65 %) des attaques de phishing prenant l'apparence de sites de e-commerce tels que eBay et Paypal.

Les attaques de phishing sont la méthode la plus courante pour obtenir des données privées – et 65 % d'entre elles sont ciblées sur les sites de e-commerce les plus importants.

Le phishing est devenu une source d'inquiétude majeure pour l'industrie, chaque attaque réussie ayant pour conséquence une perte de 220 $ en moyenne pour chaque consommateur. Le problème se répand de plus en plus : 30.000 nouveaux sites de phishing ont été identifiés chaque mois au cours de l'année 2007.

La confrontation avec les problèmes de protection de la vie privée et des données est de plus en plus difficile en raison de la diversité des organisations détenant des informations numériques sur les individus – des entreprises et sociétés (commerce, banques) aux organismes gouvernementaux et aux sites de réseaux sociaux.

Par-delà ceci, définir ce qu'est une donnée privée est un sujet dynamique qui nécessite une adaptation étant donné les évolutions technologiques (par exemple, la question de savoir si une adresse IP doit être considérée comme une données personnelle ou non fait l'objet de vives discussions). Un autre point clé est de déterminer comment un consentement peut être garanti pour permettre le partage des données. Deux modèles alternatifs sont fréquemment discutés : « opt-in » contre « opt-out ». Le premier demande aux consommateurs de consentir activement au partage de leurs données. Le modèle alternatif « opt-out » est moins répandu auprès des consommateurs étant donné qu'il se base sur un consentement implicite des consommateurs au partage de leurs données à moins que ceux-ci ne le révoquent expressément, et que cette possibilité de révocation n'est pas toujours clairement énoncée. Une transparence accrue concernant l'utilisation souhaitée des

Plus de 30.000 nouveaux sites de phishing sont identifiés chaque mois – chaque attaque réussie coûte au consommateur 220 $ en moyenne.

données personnelles permettra de minimiser de nombreuses inquiétudes dans la discussion « opt-in » contre « opt-out ».

Le cas des formes illégales d'acquisition de données telles que le phishing est plus clair pour ce qui est de déterminer qu'un crime a été commis. Cependant, la nature internationale de ce crime le rend difficile à appréhender et à poursuivre en justice. En grande majorité, les attaques de phishing sont lancées par des criminels qui ne se trouvent pas dans le même pays que les victimes et l'équipement utilisé pour l'attaque est fréquemment localisé dans un troisième pays ne disposant d'aucun système sophistiqué de lois relatives à l'Internet. En raison de ceci, il est quasiment impossible de faire appliquer les lois locales par la police.

5. PROTECTION DES MINEURS

La protection des mineurs tend à défendre le bien-être des mineurs sur Internet. Elle a quatre objectifs principaux :

1. Protéger les enfants contre toute exposition à des contenus indésirables – ceux-ci vont des contenus explicitement sexuels aux contenus violents ou aguicheurs dont les parents et la société souhaitent protéger les enfants (par ex. pornographie, violence).

2. Prévenir le harcèlement – défini comme un comportement délibérément hostile envers un mineur par un pair ou un groupe de pairs dans l'environnement numérique (par ex. « happy slapping » - le fait de gifler soudainement une personne tandis qu'un complice filme la scène -, prise et envoi de photographies humiliantes).

3. Prévenir le grooming et la sollicitation – lorsque des adultes utilisent des environnements numériques (par ex. sites de chat, sites de réseaux sociaux) pour repérer des enfants et bâtir une relation virtuelle de confiance pour obtenir ensuite un contact personnel à des fins malveillantes.

4. Lutter contre les contenus de pornographie enfantine – qui impliquent un abus sexuel d'enfants lors de la production de matériel pornographique (images, vidéos). Trois domaines principaux d'action sont impliqués : 1) poursuivre les utilisateurs de contenus de pornographie enfantine, 2) poursuivre les fournisseurs de contenus de pornographie enfantine et supprimer le matériel, 3) éviter que des utilisateurs d'Internet soient fortuitement confrontés à des contenus de pornographie enfantine.

Phishing – Explication et principales techniques utilisées

Le phishing est principalement mis en œuvre par le biais d'e-mails falsifiés ; la prévention avec des filtres anti-spam dans les programmes de mail est assez efficace mais n'est pas parfaite.

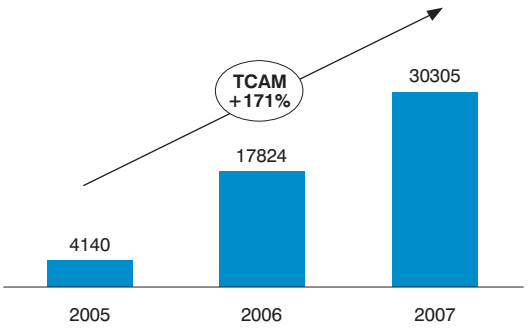
Les e-mails de phishing des débuts étaient encore réalisés de manière artisanale, avec un design et des textes peu convaincants (erreurs d'orthographe), mais ils se sont radicalement améliorés aujourd'hui – même les utilisateurs expérimentés ont du mal à voir la différence.

Le phishing est principalement basé sur deux techniques :

- **Manipulation de liens :** par exemple « g00gle.com »
- **Falsification de sites Web :** les sites phishing ressemblent au site original, et contiennent parfois l'adresse de celui-ci (grâce à l'utilisation de brèches dans la sécurité du programme de navigation)

Viser la Confiance Numérique par rapport à la protection des mineurs est un point crucial étant donné qu'il s'agit ici de la sphère la plus émotionnelle de la Confiance Numérique. Il s'agit également d'une menace très réelle : presque 20 % des jeunes ont déjà été victimes de sollicitations en ligne et 25 % ont été confrontés à des contenus indécents (voir Illustrations 30 et 31). Au sujet des contenus de pornographie enfantine, le Sydney Morning Herald a relaté en juin 2008 des chiffres effrayants en rapport avec une vague considérable d'arrestations d'utilisateurs de contenus de pornographie enfantine : 99 images insérées par un cyberpirate sur « un site Web européen respectable » ont entraîné « la somme incroyable de 12 millions de visites en seulement 76 heures après que la nouvelle de la présence des images a fait le tour des réseaux pédophiles en ligne et que l'adresse du site Web a été communiquée ».

Illustration 29 : Nombre moyen de nouveaux sites de phishing par mois (dans le monde)



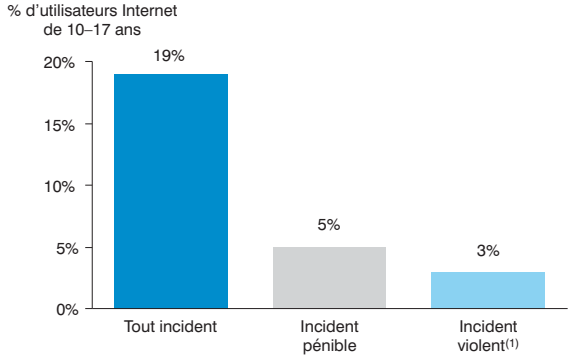
Source : PhishTank, APWG, Centre des fraudes de la NCL

Vie privée et piraterie

États-Unis, mai 2008 : Le Walter Reed Army Hospital a divulgué des informations personnelles concernant plus de 1.000 patients lors d'une violation de la sécurité. Les données étaient contenues dans un seul fichier ayant été involontairement partagé sur un système P2P.

Plusieurs autres violations de données ont déjà eu lieu en raison du partage de fichiers sur des systèmes P2P, par exemple chez ABN Amro et Pfizer. Bien que la majorité des entreprises interdisent dans leurs politiques l'usage de systèmes P2P, les utilisateurs ne sont pas conscients du danger inhérent à ceux-ci.

Illustration 30 : Sollicitation d'enfants à des fins sexuelles sur Internet (USA, 2006)



(1) Note : Incidents violents = tentatives de contacter l'enfant non seulement en ligne mais aussi par téléphone/courrier
Source : Crimes Against Children Research Centre

Cependant, l'industrie fait face à toute une série de défis. De nombreux parents gardent une distance trop importante par rapport au monde numérique et ne sont pas conscients de l'ampleur des contenus indésirables ni du niveau de sophistication des autres pratiques malveillantes en ligne telles que le grooming ou le harcèlement. En conséquence, ils n'accomplissent pas les démarches nécessaires pour surveiller et protéger leurs enfants dans les activités en ligne de ces derniers. Ceci est particulièrement pertinent dans le contexte des sites de réseaux sociaux utilisés par des adultes prédateurs.

La protection des mineurs est une véritable préoccupation ; 20 % des jeunes au Royaume-Uni ont déjà été victime de sollicitations en ligne et 25 % ont déjà été confrontés à des contenus indécents.

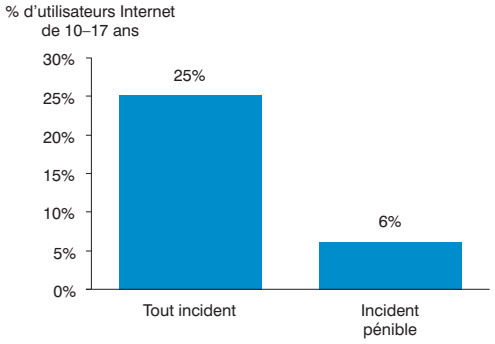
Ici se situe un autre problème dans la lutte contre cette menace : un grand nombre de ces risques est étroitement lié à la richesse des fonctionnalités des sites de réseaux sociaux, à l'anonymat des environnements numériques et à la possibilité de créer une fausse identité. Par définition, les nombreux acteurs permettant et enrichissant le monde numérique donnent par ailleurs à des activités indésirables la possibilité d'exister et menacent par là même la viabilité du monde numérique.

*32 % des adolescents aux États-Unis ont déjà constaté que leurs données privées avaient été envoyées sans leur consentement.**

Pour aborder cette sphère de menaces, il est d'abord nécessaire de la définir et de l'identifier. Tout un chacun serait prêt à approuver que les contenus de pornographie enfantine sont inacceptables et constituent une activité que toutes les parties prenantes devraient tenter d'empêcher. Au-delà de cette sphère, il y aura cependant toujours de nombreux débats et des opinions divergentes quant à savoir ce qu'est un contenu acceptable pour les mineurs et quelles formes de contenu peuvent être criminalisées, ces thèmes devant à leur tour se confronter aux questions de liberté d'expression et de libertés civiles.

*Source: Pew Internet & American Life Project

Illustration 31 : Exposition non souhaitée à des contenus pour adultes (USA, 2006)



Source : Crimes Against Children Research Centre

6. PRÉVENTION DE LA PIRATERIE ET DU VOL

La prévention de la piraterie et du vol vise à procurer un environnement commercial sécurisé pour l'économie numérique. Il a deux objectifs principaux :

1. Contrer le partage illégal de contenus sous copyright – c.-à-d. partager illégalement des contenus protégés par des copyrights par le biais d'applications telles que les réseaux pair-à-pair

2. Protéger les transactions du e-commerce – c.-à-d. s'assurer que les individus adhèrent aux standards de service habituellement en vigueur lorsqu'ils effectuent des transactions en ligne. Par exemple : non-paiement, non-livraison des biens et services convenus

Pour les entreprises et les fournisseurs de contenus, le fait d'avoir accès à des environnements de distribution sécurisés est une condition préalable et indispensable qui stimule la production et la disponibilité de contenus numériques et de contenus en ligne, et qui accélèrera en outre

la transition vers de nouveaux modèles économiques en ligne. Les services du e-commerce transactionnel doivent également être protégés contre les éventualités du non-paiement par le consommateur ou de la non-livraison de biens ou services convenus. Les fournisseurs du e-commerce transactionnel requièrent la certitude que les clients et les entreprises adhèrent, lorsqu'ils effectuent des transactions en ligne, aux standards habituellement en vigueur dans le monde hors ligne. Quant aux usagers, leur principal souci est de ne pas s'exposer à des risques de criminalisation lorsqu'ils utilisent des protocoles et des applications légitimes disponibles par le biais de leurs connexions Internet haut débit, par ex. lorsqu'ils utilisent un système de distribution de contenus basé sur le P2P.

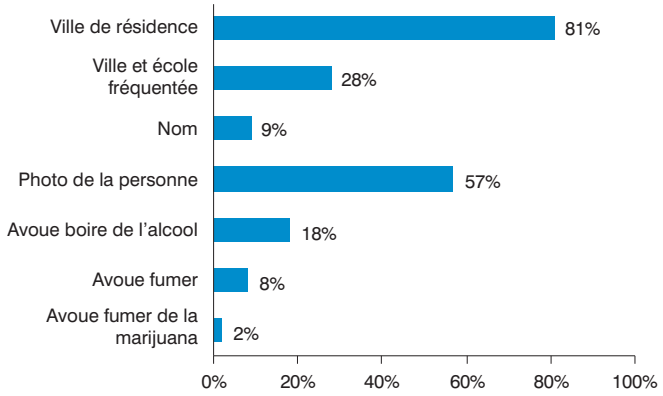
Le partage de fichiers est un réel problème pour les titulaires de copyrights – en Allemagne, le trafic pair-à-pair représente 50 % du trafic global du réseau.

PIRATERIE : PARTAGE DE FICHIERS EN PAIR-À-PAIR

Avec l'augmentation de la bande passante disponible pour les consommateurs et la numérisation des contenus, le partage de ces contenus est devenu d'une simplicité déconcertante. A la suite de Napster en tant que précurseur, des dizaines de systèmes de partage de fichiers sont aujourd'hui disponibles, la majorité d'entre eux utilisant la technologie pair-à-pair (P2P) pour distribuer les contenus. Le trafic P2P est aujourd'hui situé entre 30 % et plus de 60 % du trafic total (en fonction des régions). Lors des débuts du partage de fichiers, les fichiers partagés étaient généralement des fichiers de musique ; lorsque les réseaux haut débit se sont développés, le partage de vidéos est devenu également réalisable et représente aujourd'hui presque 80 % des contenus partagés (voir Illustration 34). Étant donné que les offres commerciales de distribution de contenus en P2P ont connu une émergence plus lente que prévu, on peut largement considérer que la majorité des contenus partagés à présent sont en réalité protégés par copyright et qu'ils sont donc partagés illicitement.

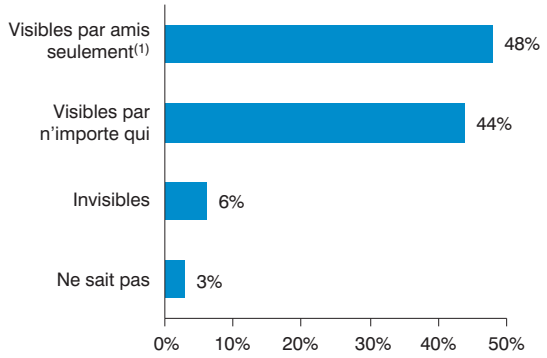
En raison de la croissance exponentielle du trafic IP principalement entraînée par les solutions P2P, la piraterie est le plus important problème déterminant le succès des nouveaux modèles économiques et le degré de développement des offres de contenus en ligne/numériques légaux. Avec l'arrivée des produits haut débit offrant des débits jusqu'à 100 Mbit/s, il est prévu que le trafic P2P (légal et illicite) reste l'un des facteurs les plus importants du trafic Internet.

Illustration 32 : Contenu des profils des jeunes utilisateurs de réseaux sociaux (Royaume-Uni, 2007)



Source : Ofcom

Illustration 33 : Visibilité des profils des réseaux sociaux (Royaume-Uni, 2007)



(1) Dans le contexte des réseaux sociaux, on entend par « ami » toute personne sur la « liste d'amis ». Il/elle n'est pas obligatoirement un ami réel ou la personne qu'il/elle dit être
Source : Ofcom

Une multitude de mesures de mitigation ont été implémentées afin de permettre une protection efficace des droits numériques par les propriétaires des contenus, avec différents degrés de succès et de controverse. Par exemple, l'usage DRM a provoqué la critique des politiciens et des associations de consommateurs en raison de l'absence de transparence dans les droits des usagers. Ceci a entraîné de fortes pressions sur les fournisseurs de réseaux et sur les FAI visant à les inciter à s'impliquer de manière plus proactive dans la lutte contre les violations de copyright. Les fournisseurs de réseaux et les FAI ne sont pas tenus de surveiller la nature de l'usage ou du trafic Internet de leurs clients sur leurs réseaux en raison du principe légal de classification de leur activité en tant que « simple tuyau ». Pourtant, nous observons que les fournisseurs de réseaux et les FAI déploient de plus en plus activement des codes autorégulateurs et des campagnes de sensibilisation afin d'éveiller les consciences et de faire comprendre la valeur du concept de propriété

Piraterie et intégrité du réseau

Au début de l'année 2007, un virus étonnamment nocif a été diffusé au Japon sur le réseau Winny, l'application P2P la plus populaire du Japon. Ce cheval de Troie raillant les partageurs de fichiers et menaçant de les dénoncer à la police voire de les tuer a effacé une multitude de types de fichiers et les a remplacés par des images de personnages de bandes dessinées célèbres les avertissant de ne pas utiliser le P2P.

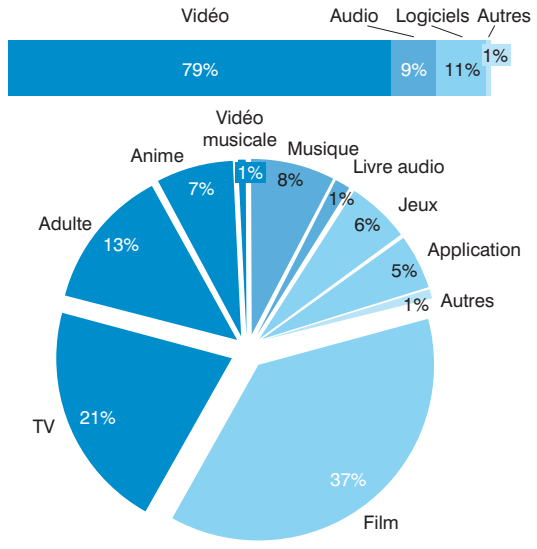
Il n'est pas illégal de programmer des virus au Japon, déclara l'auteur du cheval de Troie, un étudiant japonais qui fut ensuite arrêté pour violation de copyright parce qu'il avait utilisé dans son logiciel malveillant des graphiques de bandes dessinées sans en avoir l'autorisation.

intellectuelle parmi les membres de la génération née à l'ère du numérique qui croit majoritairement que tous les contenus en ligne devraient être gratuits. Les campagnes de sensibilisation et les codes font également l'objet de discussions parmi les mesures de mitigation dans le contexte des initiatives nationales de (co)régulation.

Les mesures potentielles envisagées dans de tels cas comprennent : la surveillance par le biais d'une vérification du trafic (Deep Packet Inspection, DPI) et/ou le filtrage des contenus ; la notification et la manipulation informatique par des autorités compétentes (applicables aux fournisseurs de réseaux proposant des contenus), la restriction ou le blocage de l'accès à certains sites ou à certains protocoles, la divulgation obligatoire des données personnelles des usagers telles que les adresses IP à des fins de poursuites, l'envoi de courriers aux détenteurs de comptes Internet lorsque leur compte a été identifié comme étant utilisé pour le partage illicite de matériel sous copyright et l'orientation des consommateurs vers d'autres sources de contenus légalement disponibles, voire l'exclusion temporaire de l'accès Internet pour les utilisateurs persistant à effectuer des téléchargements illégaux – la règle baptisée « trois attaques » ou « riposte graduée ».

Toutes ces mesures entraînent des questions importantes, telle la question de savoir comment parvenir aux meilleures pratiques en établissant un équilibre entre les objectifs anti-piraterie et les régimes existants de responsabilité légale établis pour les fournisseurs de « simples tuyaux » ; telle la question des droits fondamentaux des utilisateurs en relation avec les données personnelles et le comportement en ligne ; telle la question de la notion générale d'un Internet libre et de la liberté d'information et d'inclusion numérique. Le courant politique en Europe semble favoriser la protection des utilisateurs, à condition que ceux-ci ne tentent pas de tirer profit de leur action. La déconnexion des utilisateurs qui téléchargent est considérée comme une mesure disproportionnée allant à l'encontre des objectifs visant à atteindre une société de l'information globalisée. La mise à exécution des lois du copyright met plus fortement l'accent sur la criminalisation du téléchargement de matériel sous copyright vers un serveur que sur le téléchargement sur un ordinateur personnel, ce qui n'est même pas illégal dans toutes les juridictions. De plus, les mesures telles que le filtrage et la DPI requièrent des investissements lourds de la part des opérateurs, et la question se pose de savoir qui doit alors prendre en charge la responsabilité et subir les coûts de telles actions, par rapport au fait que la préservation des valeurs dans l'industrie des contenus peut être quantifiée et directement attribuée à de telles mesures. Par exemple, un rapport de 2007 du groupe de travail Value Recognition Strategy au Royaume-Uni, insinue que les changements de format (par ex. la « décompilation » de CD en faveur d'une sélection des chansons « à la carte » comme le pratique Apple iTunes) et la pression des prix avec des CD en vente à bas prix en supermarché sont plus responsables de la perte de valeur de l'industrie du disque britannique que les utilisateurs mettant à disposition les fichiers en P2P.

Illustration 34 : Répartition des contenus P2P (Allemagne, 2007)



Source : ipoque

7. RÉSUMÉ

Aborder les quatre piliers de la Confiance Numérique rendra possible la prochaine phase de croissance de l'industrie du numérique. Les actions déjà entreprises par diverses parties prenantes traduisent une vaste prise en considération des problèmes et de la nécessité d'agir.

BitTorrent – P2P

BitTorrent est un vrai protocole P2P largement utilisé dans la distribution de contenus. BitTorrent fonctionne sans serveur central pour les fichiers ; seul un coordination centrale - il a principalement deux tâches : (I) distribuer des fichiers torrents (serveur index, c.-à-d. juste un fichier normal/serveur Web ; le fichier torrent désigne le téléchargement torrent complet) et (II) entretenir une liste de pairs pour chaque fichier torrent (c.-à-d. si un nouveau noyau se connecte, le traqueur lui donne une liste des noyaux P2P auxquels se connecter)*.

Bien que BitTorrent soit également utilisé pour distri-buer des contenus illicites, le nombre d'usages com-merciaux est en croissance constante – et son usage légal non commercial l'est plus encore. Quelques exemples de l'utilisation de BitTorrent (sources : Wikipédia et rapports d'informations) :

- Sub Pop Records pour la distribution de musique, Vuze pour la distribution de films.
- Des services de podcast ont récemment choisi BitTorrent pour la distribution, principalement soutenue par le logiciel de lecture « Miro ».
- Amazon S3 (une solution de stockage) utilise BitTorrent pour le transfert de fichiers.
- World of Warcraft utilise BitTorrent pour distri-buer les mises à jour du jeu (plusieurs fichiers de 100 MO).
- Distribution de patchs, par ex. l'université IN-HOLLAND a distribué 22TB de patchs à 6.500 ordinateurs en seulement 4 heures – une performance quasiment impossible dans un environnement de programme mail/serveur (cela prenait 4 jours sans BitTorrent) – avec une diminution de 20 serveurs de téléchargement (auparavant 22, maintenant 2).

En raison de la croissance de cet usage, le protocole ne peut pas être « banni » de l'Internet comme cela a parfois été envisagé (afin de minimiser le partage de fichiers) ; il a été implémenté par de nombreuses universités afin d'éviter les problèmes de responsabilité avec l'industrie des médias).

* Note : BitTorrent peut également être implémenté sans serveur traqueur central, par ex. en utilisant des hashtables distribuées (de nombreuses installations soutiennent déjà ceci). Ceci permet un véritable système P2P sans serveur.

Liens de téléchargement direct (Direct Download Links, DDL) – Une alternative au partage de fichiers en P2P

- Les liens de téléchargement direct fonctionnent comme des serveurs Web normaux, c.-à-d. ils ne transfèrent pas des fichiers entre des pairs.

- Les utilisateurs peuvent créer un compte et télécharger des fichiers vers le serveur (jusqu'à plusieurs centaines de mégaoctets). Ces fichiers sont accessibles par l'intermédiaire d'un lien direct qui est seulement connu de l'utilisateur (cela signifie qu'il n'y a généralement aucune possibilité de rechercher des contenus sur le serveur DDL).

- La personne téléchargeant vers le serveur distribue maintenant le lien (normalement par le biais de forums tiers) et chacun peut ensuite télécharger des fichiers sur son ordinateur.

- Les utilisateurs sans compte payé sur le serveur DDL ont une largeur de bande limitée et un volume maximum pour télécharger vers l'ordinateur. De plus, les utilisateurs doivent attendre avant chaque téléchargement (environ 1-2 minutes pour le premier téléchargement, la durée augmentant pour les téléchargements ultérieurs sur la base du volume utilisé) et doivent remplir un captcha pour chaque téléchargement.

- Rapidshare et MegaUpload sont par exemple des solutions DDL célèbres ; ces services ne sont pas très populaires en Europe à l'heure actuelle, mais ils sont fortement utilisés au Moyen-Orient (9 % du trafic au Moyen-Orient est un trafic DDL).

Mais les parties prenantes se trouvent face à un problème multidimensionnel. Il existe par exemple d'importantes différences dans la législation des différents pays au sujet des problèmes clés, alors que les attaques numériques, notamment le phishing, sont transfrontalières et requièrent une coopération internationale en vue d'engager des poursuites. Il est souvent difficile voire impossible d'en retrouver les auteurs et d'engager des poursuites contre eux – les mesures et outils définis pour le monde « analogique » sont tout simplement inefficaces dans l'environnement numérique. De plus, il existe d'énormes zones grises en raison de l'évolution rapide des technologies, des comportements et des nouvelles possibilités offertes dans le monde numérique, qui vont de la simplicité de la duplication des biens numériques à celle de l'accessibilité à Internet dans le monde entier.

L'industrie considère largement la Confiance Numérique comme étant l'ordre du jour prioritaire mais elle se débat encore avec la question de savoir comment l'aborder efficacement.

Les organes de régulation et le gouvernement sont dans l'obligation de définir leur position et doivent trouver leur équilibre entre une législation de la main forte et l'éducation du consommateur ou l'application de philosophies libérales d'autorégulation du marché. Un rôle crucial dans la confrontation avec les problèmes de confiance numérique est également joué par la coopération internationale et par la ratification des traités internationaux pour rapprocher les législations nationales, afin de permettre la criminalisation commune des activités qui peuvent parfois sembler clairement illégales mais pour lesquelles il manque une base légale de pénalisation. Par exemple, de nouvelles propositions de loi ont été présentées très récemment seulement – en mai 2008 – au Royaume-Uni, visant à combler un vide juridique laissant jusqu'ici impunis les dessins et images de pornographie enfantine générées par ordinateur.

L'industrie se trouve confrontée au choix entre différents degrés d'intervention. Elle doit mettre en balance les exigences des nouveaux modèles économiques et des dépenses d'investissement par rapport aux inquiétudes et problèmes plus larges du public et à la nécessité d'innover et de développer des nouveaux services et des nouvelles topologies de réseau à même de prendre en compte les besoins et les valeurs de la génération née à l'ère du numérique. L'industrie est généralement préoccupée par sa propre exposition à des responsabilités légales incontrôlables et est dépendante à ce niveau des gouvernements ou des organes de régulation. Suivant le problème spécifique et le pays concerné par celui-ci, il ne peut pas y avoir d'approche « unique pour tous » dans l'objectif d'encourager la confiance numérique, mais d'importants enseignements peuvent être tirés des meilleures pratiques. L'absence d'une approche cohérente va en fin de compte au détriment du consommateur qui déplore le manque de transparence et d'assistance vis-à-vis des risques et avantages de l'économie numérique, tandis que les entreprises sont mises au défi de créer de nouveaux modèles économiques numériques novateurs et viables.

La définition des quatre piliers de la Confiance Numérique permet de structurer le problème, d'en établir les priorités et de s'y confronter

Les aspects les plus difficiles de la Confiance Numérique ne se concentrent pas autour de la question de savoir quels points doivent être abordés, mais bien de savoir comment et par qui. Il est nécessaire de définir les mesures les mieux appropriées et d'assigner les responsabilités – c.-à-d. à quel niveau l'action est requise : consommateur, entreprises, régulateur. Et un autre point crucial : qui doit payer ces actions ?

Sur la base des entretiens que nous avons menés, il apparaît que les difficultés résident moins dans les solutions technologiques que dans les problèmes des politiques fondamentales sous-jacentes : une entreprise doit-elle s'impliquer par ex. dans le blocage des contenus illégaux et indésirables, prendre le risque de responsabilités juridiques ? Si oui, qui détermine alors ce qui est illégal et en particulier « indésirable » ? Comment établir la limite par ex. en cas de blocage de contenus de pornographie enfantine, qu'en est-il du racisme ?

En fin de compte, les questions rencontrées impliquent un large spectre d'intérêts sans réponse simple. Les quatre piliers de la Confiance Numérique, tels qu'ils sont définis, ordonnent et structurent les aspects les plus importants du problème en tenant compte d'un débat et d'une confrontation larges.

FILTRAGE DE CONTENUS

Le filtrage de contenus est utilisé pour restreindre l'accès à certains sites spécifiques ou à des parties de sites sur Internet. Le filtrage du trafic ou de contenus peut être utilisé à des fins multiples et variées, par ex. pour

- Filtrer les courriels spam.
- Restreindre ou bloquer l'accès à des contenus illégaux, tels que les contenus de pornographie enfantine ou les contenus violant un copyright.
- Empêcher les mineurs d'accéder à des contenus inappropriés.

En fonction des motifs sous-jacents, les méthodes de filtrage peuvent être différentes. Généralement, il est possible de distinguer entre le filtrage basé sur l'équipement de l'utilisateur final (fréquemment utilisé dans les solutions de protection des mineurs, les parents pouvant le désactiver pour eux-mêmes), le filtrage basé sur le réseau (par ex. pour restreindre ou bloquer l'accès aux contenus illégaux) ou une combinaison des deux (par ex. pour le filtrage des spams, les serveurs e-mail filtrent le spam en se basant sur des listes noires et le logiciel client e-mail filtre le reste des spams en se basant sur leur contenu).

Pour le filtrage basé sur le réseau, il existe une multitude de méthodes présentées dans l'Illustration 35. L'implémentation la plus courante est le filtrage d'URL basé sur le DNS[4]. Dans ce cas, un certain accès à l'adresse IP dépendant d'un domaine spécifique est bloqué sur la base du nom du domaine (par ex. « www.google.com » serait

(4) DNS (Domain Name System) est le système des noms de domaines permettant à un ordinateur de trouver le serveur pour un domaine donné.

restreint, mais pas « www.google.uk » puisque ce sont des noms de domaines différents). Ce filtre peut être implémenté très facilement par chaque fournisseur de réseau et agit pour tous les clients utilisant le serveur DNS du fournisseur. Cependant, ce filtre peut être facilement déjoué par le biais d'une connexion à un serveur DNS alternatif sans filtres installés, et il est utilisable uniquement pour les contenus figurant sur des listes noires. Le filtrage DNS a néanmoins prouvé son efficacité dans la prévention des accès involontaires ou accidentels à des contenus illégaux.

Les filtres plus sophistiqués examinent le contenu réel du trafic afin de déterminer s'il doit être filtré. Un exemple simple est la détection d'e-mails spam. Dans ce cas, le serveur mail analyse le contenu de l'e-mail. Un autre exemple sont les simples « filtres de contenus pour adultes » qui scannent le texte d'un site Web en cherchant des mots clés comme « porno » et qui bloquent ensuite leur accès. La version la plus complexe de ceci sont les « filtres dynamiques d'empreintes de contenus » qui peuvent analyser le contenu du trafic audio et vidéo, par ex. pour déterminer si des fichiers protégés par copyright sont transférés. La vaste vérification de paquets (DPI), qui est la technologie nécessaire pour permettre de telles techniques de filtrage plus sophistiqué, provoque cependant certaines controverses. La DPI permet une surveillance du trafic individuel sur une base « frappe par frappe » pouvant également inclure la correspondance e-mail. La DPI a fait croître les inquiétudes relatives à la vie privée - étant donné qu'elle permet la collecte de données personnelles (sites Web visités, recherches) - et les inquiétudes par rapport aux interceptions illicites.

Le blackholing est un filtrage très simple mais extrêmement efficace, bien que contenant cependant certains défauts significatifs. Le blackholing bloque l'accès complet à une adresse IP donnée (les paquets destinés à cette adresse ne sont pas envoyés) et s'avère difficile à contourner, même pour les usagers expérimentés du Web. Mais étant donné que plusieurs systèmes et sites Web peuvent être localisés sur la même adresse IP, le blocage d'une IP est susceptible de bloquer des centaines de sites Web ou d'utilisateurs, provoquant ainsi un « dommage collatéral » (appelé un surblocage). De ce fait, il s'agit ici d'une mesure utilisée uniquement lorsque l'intégrité de larges réseaux est compromise ou lorsque les utilisateurs encourraient un risque élevé sans le blackholing.

Les mesures de filtrage en général ne peuvent être efficaces que lorsque des listes de contenus illégaux sont établies, entretenues, régulièrement actualisées et mises en application. De larges implications relatives au public sont cependant en jeu si les listes sont amenées à être élargies au-delà de leur objectif d'origine, ou dans les cas où les contenus illégaux ne sont pas retirés à l'intérieur d'un délai approprié.

Illustration 35 : Outils de filtrage du trafic web

	Filtre URL basé sur proxy	Filtre URL basé sur DNS	Filtre dynamique d'empreinte digitale de contenu	Filtre mots clés de contenu	Blocage IP/ "Blackholing"
Description	Analyse et comparaison de l'URL de la requête avec liste noire/ blanche	Liste noire des entrées DNS de domaines spécifiques et reroutage	Vérification (DPI) et empreinte digitale (ex. identification du contenu) du contenu de paquets	Vérification (DPI) et détection des mots clés du contenu de paquets – http/ smtp seulement	Blocage d'adresses IP sélectionnées dans routeurs (frontière et interne possible)
Impact du filtrage	Précis/ciblé → Nombre de sites concernés				
	Une seule page	Un seul site/domaine	Contenu correspondant à l'empreinte digitale	Toutes les pages/URL contenant le mot clé	Tous les sites/appareils localisés à cet IP
	★★	★★★	★	★★	★★★
	Serveur proxy nécessaire	Configuration DNS	DPI complexe et base données de contenu nécessaire	DPI nécessaire	Configuration routeur
Pour/Contre	Moins facile à contourner que filtrage DNS, mais plus grande complexité technique et problème de volume de trafic	Filtre facile à contourner avec modifications de la configuration DNS locale	Contenu peut être détecté, mais décision sur utilisation légale impossible	Surblocage en fonction du mot clé, contourné par encryptage	Surblocage extrême avec NAT/ hébergement partagé, contourné par tunneling
Exemple		Blocage de sites basé sur liste noire (ex. blocage ThePirateBay au Danemark)	Détection de fichiers audio protégés par copyright lors du partage de fichiers	Filtres simples pour PC, blocage de tous les sites contenant le mot "sexe"	Utilisation du blackholing pour protéger les réseaux et appareils du déni de service

Note : Non exhaustif, p.ex. utilisation du blocage de port en plus du filtrage DNS pour rendre le contournement plus difficile

Source : Booz & Company

★ Implémentation difficile/chère

★★★ Implémentation simple/bon marché

IV. APPROCHE ACTUELLE DE LA CONFIANCE NUMÉRIQUE : MARGE D'AMÉLIORATION CONSIDÉRABLE

Pour développer un cadre cohérent assurant la Confiance Numérique, il est essentiel de reconsidérer les approches de diverses parties prenantes afin d'aborder les défis ayant des priorités croissantes tout autour de la Confiance Numérique.

La discussion se porte sur un ensemble d'études de cas afin de comprendre les meilleures (et les pires) pratiques et d'en tirer des enseignements pour pouvoir continuer à avancer. La considération des études de cas est ensuite complétée par un bref passage en revue des points à traiter par le régulateur en rapport avec la Confiance Numérique.

1 ÉTUDES DE CAS : COMMENT FAIRE FONCTIONNER LA CONFIANCE NUMÉRIQUE DE MANIÈRE RÉUSSIE – OU NON

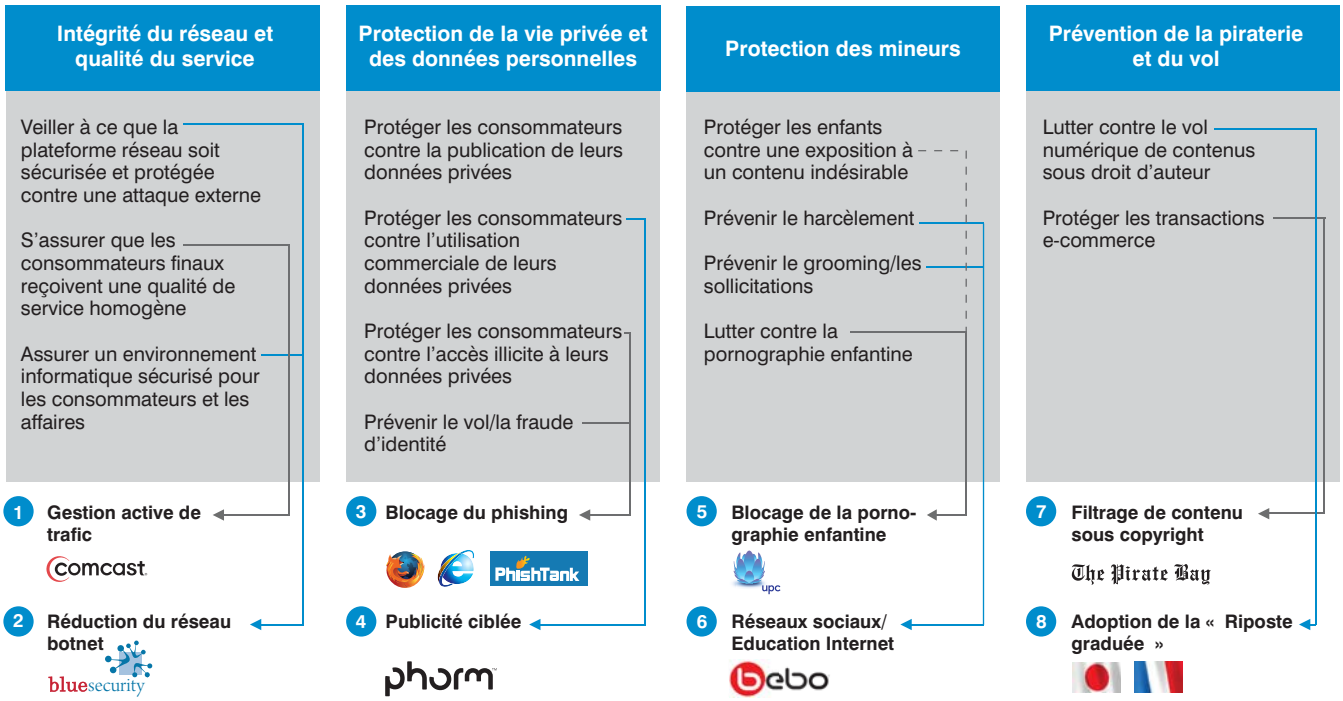
Les cas ont été identifiés autour des quatre piliers de la Confiance Numérique – intégrité du réseau et qualité du service, protection de la vie privée et des données, prévention de la piraterie et du vol et protection des mineurs. Deux cas par pilier ont été choisis afin d'illustrer autant que possible les objectifs de chaque pilier et afin de permettre des conclusions perspicaces (Illustration 37) :

- « Potentiel d'enseignement ».
- Opportunité.
- Diversité géographique.

Comme établi au chapitre III, l'une des questions clés est la position générale prise par les entreprises dans chaque domaine spécifique de la Confiance Numérique : quel degré de protection voire de prescription voudrais-je – ou dois-je – appliquer ? Jusqu'où peuvent aller les mesures mises en place ?

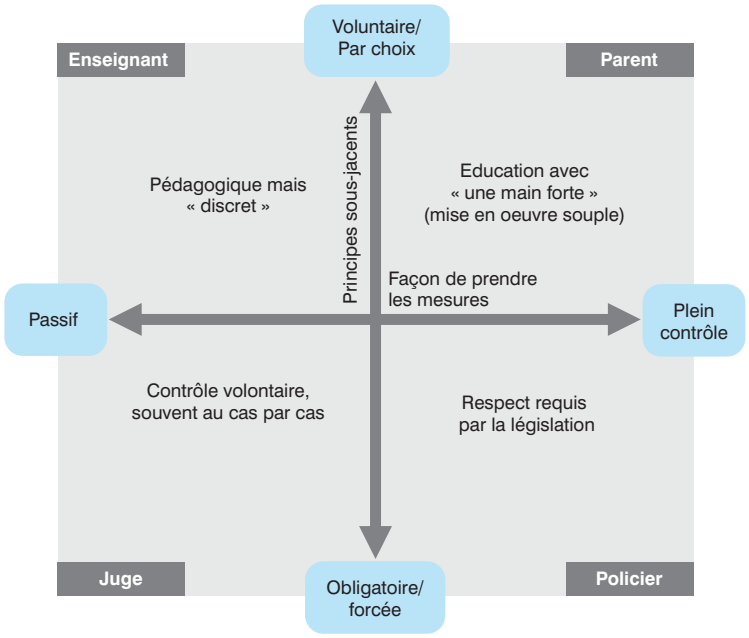
Pour examiner les cas, un « cadre de positionnement de la Confiance Numérique » générique a été développé (Illustration 36). À l'intérieur de ce cadre, l'axe horizontal représente la manière dont sont prises les mesures (par ex. passivement selon le principe de la « non-intervention » ou

Illustration 36 : Approches actuelles—quelques cas



Note : Les couleurs des flèches servent uniquement à distinguer les cas
ligne pleine = aspect important du cas ; ligne pointillée = aspect moins important

Illustration 37 : Matrice de la Confiance numérique



activement selon une méthode de « plein contrôle »), tandis que l'axe vertical distingue les principes sous-jacents. Les quatre cadrans en résultant peuvent être clairement reliés à des rôles sociétaux génériques. Par exemple :

- L'Enseignant éduque autant que possible les utilisateurs au sujet des opportunités et des menaces, mais ne prendra normalement aucune mesure corrective active (par ex. « Web Wise Kids » produisant du matériel éducatif pour les enfants sur Internet).

- Le Parent éduque les utilisateurs au sujet des menaces et des mesures de manière similaire à l'Enseignant, mais prendra des mesures de manière proactive si cela est jugé nécessaire pour protéger les utilisateurs (par ex. YouTube filtrant les contenus protégés par copyright).

- Le Juge se base sur une mise en application auto-imposée de règles au cas par cas et sur des directives plutôt que sur l'éducation, mais les règles sont basées sur des accords mutuels (par ex. UPC NL restreignant de manière proactive l'accès aux domaines ayant des contenus de pornographie enfantine).

- Le Policier est naturellement enclin à une mise en application forte basée sur le mandat légal, il prend toutes les mesures nécessaires et agit en se basant sur des règles strictes, par ex. en bloquant toutes les activités illégales (par ex. l'implémentation d'une règle de « riposte graduée et vous êtes dehors » en cas de violation du copyright).

CAS 1 : GESTION ACTIVE DU TRAFIC

***Problème :** Les fournisseurs de réseaux se trouvent face à un usage croissant de bande passante et doivent gérer le trafic du réseau afin d'éviter une congestion et d'assurer la qualité du service*
***Risque :** La qualité du service est susceptible d'être affectée par des surcharges de la demande sur les réseaux haut débit – mais une seule actualisation de la bande passante s'avérerait d'un prix prohibitif tout en ne fournissant pas de solution à long terme*

Les utilisateurs lourds consomment une grande quantité de bande passante aux dépens des utilisateurs ordinaires. Les applications telles que le partage de fichiers et le streaming de vidéos nécessitent une bande passante beaucoup plus considérable que la navigation standard sur le Web ou la correspondance e-mail. Cette variation d'intensité se traduit par de fortes pointes dans l'utilisation de la capacité globale de certains réseaux donnés. Les fournisseurs de réseaux abordent ce problème en investissant dans des réseaux d'accès de nouvelle génération afin d'élargir continuellement la capacité disponible pour les utilisateurs finaux. Mais pour garantir que tous les clients obtiennent une qualité de service (QdS) optimale, un élargissement de la capacité n'est pas suffisant à lui seul. Il existe un ensemble croissant d'utilisateurs lourds utilisant une quantité croissante de bande passante, ce qui signifie que des augmentations des capacités ne seraient à elles seules qu'une solution de court terme pour résoudre les défaillances de bande passante. De ce fait, il est également nécessaire de gérer le trafic afin de garantir une répartition « équitable » dans la consommation de bande passante et d'assurer la QdS pour tous les utilisateurs (Illustration 39). Dans l'environnement des tarifs forfaitaires, les utilisateurs ayant une forte consommation (part importante de la courbe) sont en quelque sorte « subventionnés » par les utilisateurs ayant une faible consommation. Illustrons ceci : si le trafic de 10 % des utilisateurs téléchargeant le plus était contrôlé ou redirigé vers des niveaux d'usage supérieurs, l'équité dans la répartition de la bande passante disponible pour tous les usagers croîtrait alors de presque 50 %.

Un échelonnage des prix et des mesures de gestion du trafic sont les deux remèdes essentiels. L'échelonnage des prix pourrait inciter les utilisateurs lourds à réduire leur usage du réseau

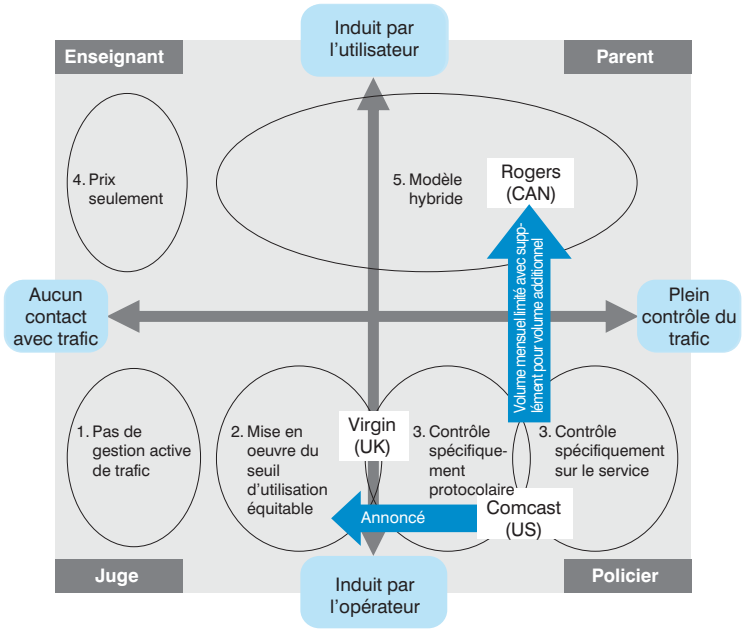
par le paiement de suppléments lors de téléchargements pendant les heures de pointe, notamment pour les applications nécessitant une bande passante importante telles que le partage de fichiers. Ces suppléments ont deux effets : premièrement, ils déplaceront la demande hors des heures de pointe et deuxièmement, ils se traduiront par des recettes supplémentaires pouvant contribuer à couvrir les coûts d'élargissement des infrastructures. L'opérateur câble canadien Rogers a introduit des prix échelonnés, AT&T aux États-Unis est en train d'évaluer un modèle de prix spécial pour le trafic BitTorrent afin de réduire l'impact du trafic P2P sur le réseau (l'entreprise prévoit que l'utilisation totale de la bande passante sur son réseau quadruplera au cours des trois prochaines années), et Time Warner est en train de tester un système de prix au volume qui fait payer aux utilisateurs la quantité de bande passante consommée.

Les mesures de gestion du trafic englobent une vaste gamme de mesures menées sur le réseau et visant à faciliter le flux du trafic ainsi qu'à garantir la qualité du service – pour accroître les dimensions générales du réseau, notamment afin de gérer les heures de pointe. Ces mesures vont de la mise en vigueur de limites d'usage équitable à des formes variées de contrôle du trafic et à l'implémentation de différentes méthodes de sélection du trafic pour garantir la meilleure QdS possible (voir également le chapitre III).

Les méthodes employées par les acteurs pour gérer le trafic peuvent être discutées en se référant à une version adaptée du cadre générique de positionnement de la Confiance Numérique (Illustration 38). L'axe vertical différencie la position générale pouvant être adoptée par un opérateur de réseau ou FAI par rapport à la gestion de trafic. Sur cet axe, l'extrémité supérieure est une position qui émet une incitation mais qui n'interfère pas dans l'activité réelle de l'utilisateur, tandis que l'extrémité inférieure est une position de contrainte qui réagit activement et qui gère le trafic sur la base de l'activité globale de l'utilisateur à un moment donné. L'axe horizontal différencie le degré selon lequel les données réelles du trafic déterminent les actions à entreprendre, c.-à-d. le degré de spécificité des mesures techniques employées. Par exemple, le contrôle spécifique au service distingue entre des types variés de trafic à un niveau plus cristallisé que le contrôle spécifique au protocole.

Certaines positions sur cette matrice sont plus naturelles que d'autres : par exemple, une approche « par les prix seulement » comme dans le cadran de l'Enseignant est une approche assez improbable étant donné le déséquilibre actuel entre la disponibilité de la bande passante et la demande – les opérateurs de réseaux ne peuvent pas garantir le bon fonctionnement du réseau sans aucune mesure technique de gestion du trafic.

Illustration 38 : Matrice de la Confiance Numérique—gestion active du trafic



1. Seuls peu d'opérateurs de réseaux ne gèrent pas activement leur trafic
   – Pour : tant que la capacité est suffisante, aucun besoin réel de gestion active du trafic
   – Contre : aucune expérience garantie des utilisateurs – congestion potentielle du réseau
2. La majorité des opérateurs de réseaux ont mis en place des stratégies « d'utilisation équitable », basées sur le dimensionnement du réseau et dont le but est de gérer les heures de pointe de la consommation
   – Les utilisateurs excédant les limites de l'utilisation équitable peuvent être migrés vers des abonne-ments haut débit alternatifs (bande passante plus élevée)
3. La gestion active de trafic est déployée pour garantir la qualité du service pour tous les utilisateurs
   – D'un point de vue de neutralité du Net, une approche non spécifique de protocole est préférable à une approche spécifique de service
4. Une alternative à la gestion de la bande passante induite par le commerce est basée sur l'utilisation, avec différents tarifs
   – Pour : motivation axée sur le marché pour gérer la congestion en démotivant l'utilisation excessive
   – Contre : utilisation moins pratique – désavantage compétitif potentiel
5. Des modèles hybrides (« stratégie utilisation supplémentaire ») font appel à différents tarifs lorsque la consommation excède certains seuils/plafonds
   – L'utilisateur moyen continue de bénéficier d'un « forfait » – seuls les grands utilisateurs paieront en fonction de l'utilisation

Un certain nombre de pratiques récentes se détachent de la matrice. Comcast, l'un des plus grands opérateurs câble des États-Unis, s'est trouvé confronté à une augmentation considérable du trafic en raison de l'usage accru des systèmes P2P. Face à cette pression, Comcast a renforcé sa gestion du trafic et s'est vu confronté à la résistance du public. Rogers, au Canada, a introduit des primes à l'usage, faisant payer des suppléments pour le trafic dépassant certaines limites (limite de 2 à 100 GO par mois). Ceci est un exemple d'approche hybride combinant la gestion du trafic et l'échelonnage des prix. Par ailleurs, Virgin Media au Royaume-Uni est un exemple d'opérateur câble très ouvert sur ses activités de gestion du trafic.

*« Les réseaux non gérés entraîneront une sérieuse dégradation de la disponibilité et de la qualité du service pour tous les usagers, ceci signifiant également que les clients paieront plus pour une prestation moindre, étant donné que les fournisseurs sont obligés d'élargir continuellement leurs réseaux pour rester maîtres de la croissance massive dans la consommation de bande passante. »**

Comcast a implémenté des mesures de gestion du réseau ayant un impact sur le trafic P2P de BitTorrent qui ont entraîné des résultats trop restrictifs : le téléchargement BitTorrent vers l'ordinateur était possible, mais les utilisateurs ont rapporté que les téléchargements vers le serveur étaient retardés et que l'implémentation affectait également d'autres applications nécessitant une gestion rapide ou en temps réel telles que Lotus Notes. Les plaintes d'utilisateurs individuels ont pu attirer l'attention du large public, entraînant ainsi une enquête de la FCC. Comcast a également été accusé de promesses mensongères concernant le service et de fraude informatique. En réponse à cela, Comcast se consacra très minutieusement au problème, coopéra avec BitTorrent et trouva finalement une solution mutuellement acceptable : désormais, Comcast utilisera une technique non spécifique aux platesformes susceptibles de ralentir le trafic P2P uniquement chez ses utilisateurs les plus lourds. Cet accord semble obtenir l'approbation des partisans de la neutralité du net. Au sujet de l'engagement de Comcast en faveur d'une approche de gestion du réseau non spécifique au protocole, Google a parlé « [d']un pas dans la bonne direction ». Celui-ci n'a cependant pas apaisé la FCC qui a décidé d'aller de l'avant en prenant une décision dénonçant les pratiques antérieures Comcast.

*« Ainsi, la véritable question se posant par rapport aux réseaux haut débit actuels n'est pas de savoir s'ils ont besoin d'être gérés, mais plutôt comment ils doivent l'être. »***

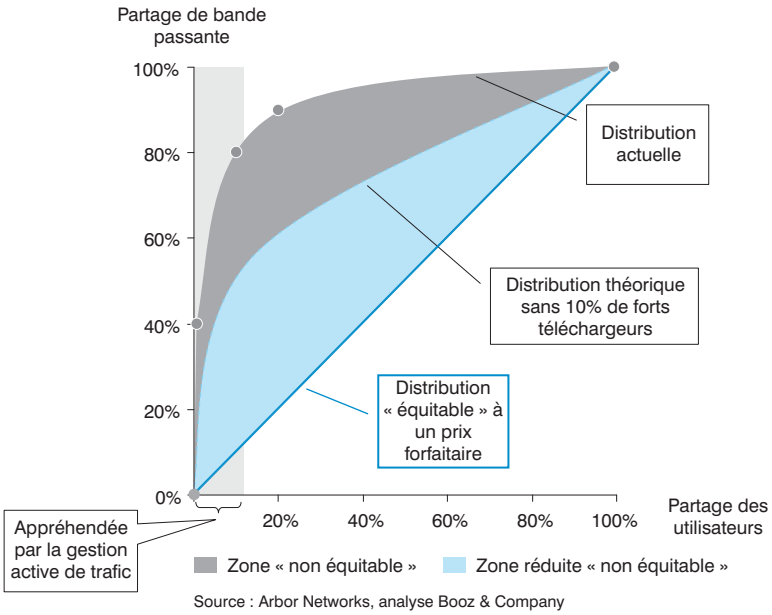
Tout en reconnaissant la nécessité d'une gestion « raisonnable » du réseau, la FCC a allégué que Comcast avait bloqué l'accès à Internet de manière arbitraire sans prendre en compte le niveau du trafic et omis de révéler cette pratique aux consommateurs. En juillet 2008, le président de la FCC a recommandé une action d'exécution, exigeant que Comcast stoppe ses « pratiques de blocage » (bien que le terme de « retardement » soit probablement une meilleure description desdites pratiques), qu'il fournisse aux consommateurs des détails de l'étendue et de la manière dont ces pratiques avaient été employées et qu'il révèle aux consommateurs les détails des plans futurs de gestion de son réseau. Cette action entre dans le cadre d'une déclaration de politique de la FCC publiée en septembre 2005 et définissant un ensemble de principes visant à garantir que les réseaux haut débit soient « largement déployés, ouverts, abordables et accessibles à tous les consommateurs » – ces principes étant cependant « sujets à une gestion raisonnable du réseau ». La décision de la FCC concernant Comcast semble plutôt être une affirmation de principe, également en raison du fait qu'il est improbable que Comcast fasse l'objet de poursuites, et paraît essentiellement vouloir établir un précédent en spécifiant plus précisément ce que signifie une « gestion raisonnable du réseau » dans la pratique.

Certains acteurs comme Virgin Media ou Rogers pratiquent une grande transparence au sujet de leurs méthodes de gestion du trafic – l'acceptation par le client semble élevée.

**Kurt Dobbins, Arbor Networks*

***Vint Cerf, Chief Internet Evangelist, Google*

Illustration 39 : Consommation de bande passante par groupes d'utilisateurs



Source : Arbor Networks, analyse Booz & Company

Rogers a introduit des suppléments de frais à l'usage en mars 2008. Les utilisateurs doivent payer un supplément de 1,25 $ à 5 $ par mois en fonction de leur programme tarifaire, avec un plafonnement à 25 $ maximum dans tous les programmes tarifaires. Un nombre croissant de fournisseurs de réseaux a commencé à prendre en considération l'introduction de modèles de prix basés sur l'usage pour gérer la demande croissante de bande passante. La difficulté dans cette approche échelonnée est qu'elle est susceptible d'ébranler la promesse d'un « prix forfaitaire » qui avait été un facteur clé du développement du marché de masse de l'Internet haut débit, c.-à-d. un usage insoucieux du réseau haut débit sans avoir à se préoccuper de coûts majorés dus à un usage difficile à surveiller. C'est ce point qui est abordé par Rogers avec le plafonnement de 25 $. La société Rogers elle-même est très ouverte et sans prétention au sujet de sa politique, et affirme sur son site Web : « La majorité de nos clients souscrit à des programmes tarifaires qui répondent à leurs besoins et qui leur permettent en principe de ne pas dépasser leur forfait d'usage mensuel. Si vous le dépassez malgré tout, vous pouvez payer l'usage supplémentaire sur une base mensuelle ou bien modifier votre niveau de service de telle sorte qu'il réponde à vos besoins en ligne. Cette manière de mesurer l'usage reflète plus équitablement la façon dont nos clients utilisent le service et nous permet de maintenir des prix mensuels concurrentiels pour tous nos clients.»

Au Royaume-Uni, Virgin Media se montre également très ouvert en ce qui concerne la nécessité d'une gestion du trafic et l'implémentation choisie. Actuellement, Virgin utilise le contrôle de trafic pour gérer les 3 % d'utilisateurs les plus lourds – les règles employées sont ouvertement communiquées au public sur le site Web. Virgin Media place ses mesures dans le contexte d'une politique d'usage équitable permettant de sauvegarder la qualité du service pour la vaste majorité des usagers. Virgin réfléchit également à l'introduction future de modèles basés sur des prix échelonnés.

De plus en plus, la gestion du trafic entraîne un nombre croissant d'examens et de régulations. La décision de la FCC dans le cas de Comcast souligne le fait que la protection des consommateurs a pour elle une priorité élevée dans le contexte visant à définir ce qui constitue une gestion « raisonnable » du trafic. Mais le sujet est complexe, également du point de vue de la régulation. Les Illustrations 40 et 41 illustrent quel genre d'impact économique pourraient avoir les décisions régulatrices dans ce contexte. Le fait d'imposer pour la qualité du service des régulations très strictes ayant un impact sur l'ampleur d'implémentation de la gestion du trafic pourrait signifier des coûts supplémentaires considérables pour l'industrie en Europe. Étant donné que les coûts ne peuvent pas être entièrement assumés par les fournisseurs de réseaux, ceux-ci seraient contraints de recouvrer ces coûts par le biais de prix plus élevés appliqués aux consommateurs finaux. L'usage excessif par un segment restreint de clients pourrait finalement entraîner une augmentation générale des prix appliqués aux consommateurs finaux. C'est la raison pour laquelle une action régulatrice dans le domaine de la gestion du trafic doit être pesée avec grand soin.

ENSEIGNEMENTS CLÉS

Cinq enseignements clés ressortent de la discussion :

- La gestion de la congestion du réseau et des contraintes de capacité est un point essentiel pour chaque opérateur de réseau - les mesures d'échelonnage des prix et de gestion du trafic sont les deux remèdes majeurs.

- Une croissance de l'usage est prévue dans le même rythme que l'augmentation de la bande passante sur les réseaux d'accès de nouvelle génération. Ceci accroît encore l'importance de la question, sachant qu'une croissance de l'usage lourd par les applications nécessitant une grande bande passante est également attendue. La facturation de suppléments pour l'usage lourd pourrait contribuer à un meilleur équilibre des flux de trafic et à une répartition équitable de la bande passante disponible entre tous les usagers.

- Les mesures de gestion du trafic sont toujours nécessaires à un certain degré et sont aptes à garantir la qualité du service dans les différents types de trafic ; la transparence vis-à-vis du public au sujet de ces pratiques est nécessaire pour gérer les attentes envers le service.

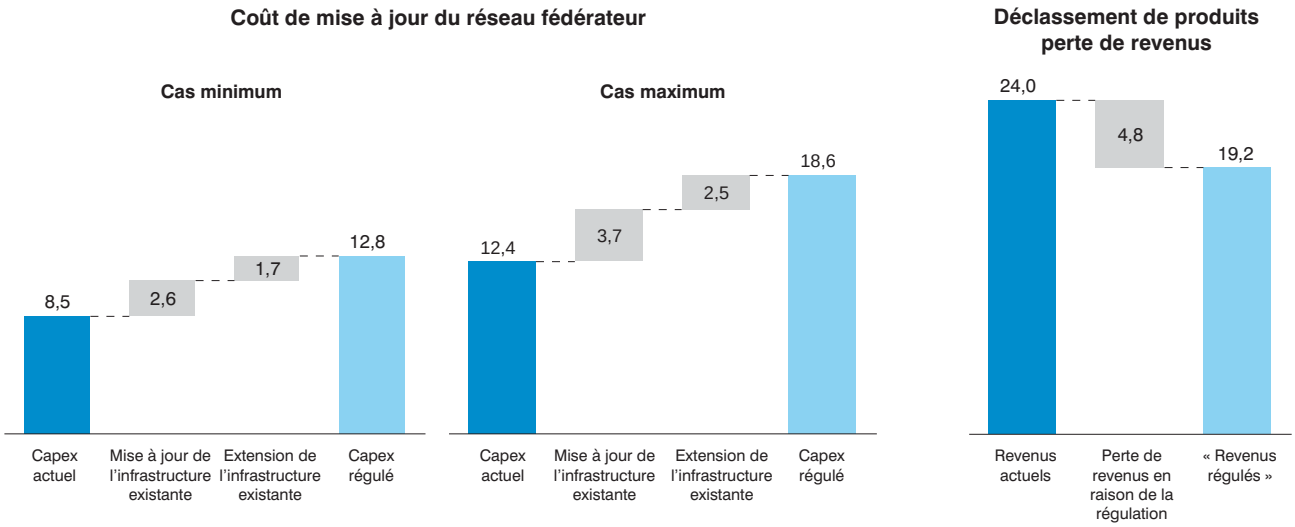
- L'implémentation de mesures de gestion du trafic doit prendre en considération les discussions quant à la neutralité de l'Internet – les implémentations spécifiques au protocole (comme BitTorrent) se sont avérées être vivement critiquées par le public. La mise en application d'un « usage équitable » non spécifique au protocole semble de ce fait être la plus équitable lorsqu'elle gère les comportements disproportionnés dans l'usage et lorsqu'elle est directement destinée et limitée à la gestion du niveau de trafic uniquement aux moments de réelle congestion. Cette approche est susceptible d'apporter la meilleure qualité de service globale ainsi qu'un niveau d'intervention proportionné à la neutralité du net.

IMPLICATIONS DE QUELQUES ALTERNATIVES DE RÉGULATION DES EXIGENCES QDS MINIMALES

Illustration 40 : Ampleur d'une régulation possible de la qualité du service

0. Aucun contrôle autorisé	1. Faibles exigences QdS	2. Exigences moyennes QdS	3. Exigences élevées QdS
• La neutralité du Net peut être interprétée comme une interdiction de contrôle du réseau • Peut être combiné avec d'autres options, mais difficile à réaliser	• Peut être mis en oeuvre en configurant les solutions de gestion de réseau existantes – Contrôle du service/protocole – Contrôle plus ou moins agressif	• P. ex. bande passante minimum ou exigences de latence modérées • Peut être implémenté avec l'infrastructure existante et de petites mises à jour – Mises à jour du réseau fédérateur pour accroître la bande passante et diminuer le contrôle – Mises à jour des accès (nouveau CPE)	• Exigence élevée QdS (bande passante minimum, combinée à une faible latence et gigue) • Réseau existant non suffisant pour répondre aux exigences, implémentation de nouvelles technologies requise
• ORMS, contrôle actuellement mis en oeuvre, deux options – Mise à jour du réseau fédérateur – Déclassement des produits	• Mise à jour du réseau fédérateur/accès pas nécessaire	• Mises à jour du réseau fédérateur/accès requises pour parties du réseau • Diffère pour DSL et opérateurs câble pour des raisons techniques (p. ex. câble avec réseau d'accès mutualisé peut fournir plus de bande passante, mais aussi plus enclin à la congestion)	• Mises à jour réseau fédérateur/accès nécessaires (reconstruction du réseau)
Déclassement de produits ou mise à jour réseau	**Aucune mise à jour**	**Mise à jour réseau**	**Réseau « reconstruit »**

Illustration 41 : Impact financier d'un règlement « aucun contrôle » en Europe (milliards d'euros)



Note : Europe UE-27 + Norvège + Suisse
Note : Scénario hypothétique selon lequel le contrôle n'est pas autorisé en Europe alors que 20% de l'ensemble du trafic et 67% de la croissance du trafic p.a. sont contrôlés (aucune hypothèse de distribution de contrôle entre les acteurs)
Source : US BEA, Merrill Lynch, Ofcom, rapports de groupes, analyse Booz & Company

• Les questions liées à la gestion du trafic pourraient être efficacement réglées par la conclusion d'accords transparents et mutuellement acceptables entre les opérateurs de réseaux et, par ex., les fournisseurs d'applications. Le niveau de la concurrence haut débit sur un marché donné devrait déterminer le besoin d'une intervention régulatrice.

CAS 2 : MITIGATION DES BOTNETS

Problème : de plus en plus d'ordinateurs de consommateurs sont infectés par des bots, des logiciels malveillants qui peuvent être contrôlés à distance par des personnes criminelles (les « bot herders ») : les FAI veulent supprimer les bots de l'Internet afin de protéger les consommateurs et les réseaux

Risque : les botnets sont la source principale de la majorité des attaques numériques telles que le phishing, le spamming, le clic fraude, etc.

Les botnets sont probablement la forme la plus grave de violation de l'intégrité des réseaux à des fins criminelles : un botnet est un ensemble de terminaux constitués d'ordinateurs personnels installés dans des domiciles privés, des entreprises, des universités, etc., et contrôlés à distance par une tierce personne non autorisée et malveillante sans que les propriétaires des ordinateurs en soient conscients. Les botnets peuvent se composer de plusieurs centaines de milliers d'ordinateurs.

Les botnets peuvent être utilisés à plusieurs fins, par ex. pour des attaques de spamming et de déni de service (DdS)[5] ou pour le phishing et la clic-fraude. Plusieurs exemples récents montrent quelles conséquences catastrophiques peuvent avoir des attaques DdS exécutées par les botnet. En avril 2007, suite à l'enlèvement d'une statue russe à Tallinn, la capitale de l'Estonie, une attaque DdS « manuelle » a été organisée : des bloggeurs ont demandé à leurs lecteurs de « pinguer » certains services estoniens spécifiques afin de créer un DdS. Un ping est une utilité logicielle qui envoie un paquet à une adresse IP spécifique pour déterminer si l'adresse est disponible. Ceci est primairement utilisé pour concilier des connexions Internet, mais il est possible d'en abuser de la manière décrite. Après avoir échoué avec cette attaque, un botnet a été « loué » et une « vraie » attaque DdS a été lancée. Les cibles de l'attaque incluaient les sites Web de la présidence estonienne et de son parlement, presque tous les ministères gouvernementaux du pays, les partis politiques, trois parmi les six grandes institutions d'information du pays, deux des plus grandes banques et des sociétés spécialisées dans la communication. L'attaque a littéralement « démonté » l'industrie du numérique dans un pays où par ex. 90 % des transactions bancaires sont effectuées en ligne.

En avril 2008, Radio Free Europe, une organisation privée non lucrative financée par les États-Unis, a subi une attaque DdS massive. Plusieurs sites Web de Radio Free Europe en Europe de l'Est ont été attaqués par un DdS en étant inondés de fausses requêtes (entraînant l'utilisation de toutes les ressources par l'attaque DdS). Ces deux attaques ont des motifs essentiellement politiques et ont été réalisées par des botnets (fréquemment « loués »).

Étant donné que la majorité des buts des botnets sont illégaux ou ont des motivations - sinon des conséquences - délictueuses, la poursuite par la mise en vigueur de lois joue un rôle central dans la lutte contre les botnets. Aux États-Unis, le FBI a mené une opération appelée « Rôti de Bots » au cours de l'été 2007, pouvant ainsi identifier environ un million d'ordinateurs ayant été compromis aux États-Unis et inculper de nombreux individus de crimes informatiques ou de cybercrimes. En dehors des poursuites, les stratégies de mitigation contre les botnets sont malheureusement limitées – la prévention contre l'infection est, la plupart du temps, efficace mais difficile.

Kraken est l'un des grands botnets connus*

**500.000 ordinateurs infectés*
50 entreprises Fortune-500 affectées

(5) Note : dans ce document, nous utilisons le terme DdS mais techniquement parlant, les attaques de botnets sont des attaques DDoS (Distributed Denial of Service attacks).

Le P4P comme moyen d'atténuer une partie du tra-fic P2P tout en améliorant la qualité du service pour les utilisateurs

P4P est la « participation proactive du fournisseur de réseaux pour le P2P », une initiative de la DCIA (Association des industries informatiques). Les membres du groupe de travail central sont divers leaders de pensée de toute l'industrie concernée : AT&T, BitTorrent, Cisco, Joost, Pando, Telefonica, Verizon, Vuze.

Le P4P a deux buts de développement : (I) diminuer le trafic vertébral, et (II) réduire les coûts d'opération des réseaux. L'idée technique derrière ceci est de construire un système P2P (basé sur BitTorrent) qui utilise l'information additionnelle sur la topologie des réseaux pour sélectionner les pairs avec lesquels des données sont échangées. Pour soutenir ceci, des serveurs traqueurs supplémentaires sont entretenus par le FAI, permettant de trier les pairs disponibles en se basant sur les routes optimales.

De plus, l'idée de caches au niveau du FAI a été introduite – permettant la réduction du volume de données dans le backhaul et l'accès (les logiciels clients ont seulement besoin d'effectuer un téléchargement des données vers le cache, le cache peut satisfaire toutes les demandes vers le réseau). Des premiers tests avec Pando (basé sur BitTorrent) présentent une augmentation de la vitesse de transmission de 200 % à 800 % avec une diminution de 40 % à 75 % du transfert de données inter-FAI.

Les méthodes de mitigation « sans poursuite » des botnets peuvent être structurées suivant une version adaptée du cadre générique de positionnement de la Confiance Numérique (Illustration 50). L'axe vertical différencie l'endroit où la mitigation a lieu : soit du côté de l'utilisateur final, soit du côté du réseau. L'axe horizontal différencie la force de l'intervention. L'extrémité gauche signifie la non-intervention totale, l'extrémité droite est une position fortement interventionniste.

L'éducation est un exemple clair de mesure non-interventionniste et centrée sur l'utilisateur : elle vise à garantir que les utilisateurs finaux comprennent les risques des botnets et sachent que faire pour y lutter. Par exemple, l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information) a publié du matériel éducatif pour les consommateurs au sujet des botnets, de leurs menaces et des méthodes à la disposition des consommateurs pour s'en protéger.

Une autre mesure rencontrée dans le cadran de l'Enseignant est l'utilisation de logiciels qui protègent les ordinateurs contre une infection par des bots. Presque tous les produits commerciaux anti-virus et pare-feu actuels contiennent des fonctions visant à prévenir les infections par des bots. Les fournisseurs de tels logiciels eux-mêmes sont également vulnérables : Blue Security, une petite entreprise consacrée aux logiciels de sécurité Internet, a été véritablement mise hors service par une attaque DdS massive en mai 2006.

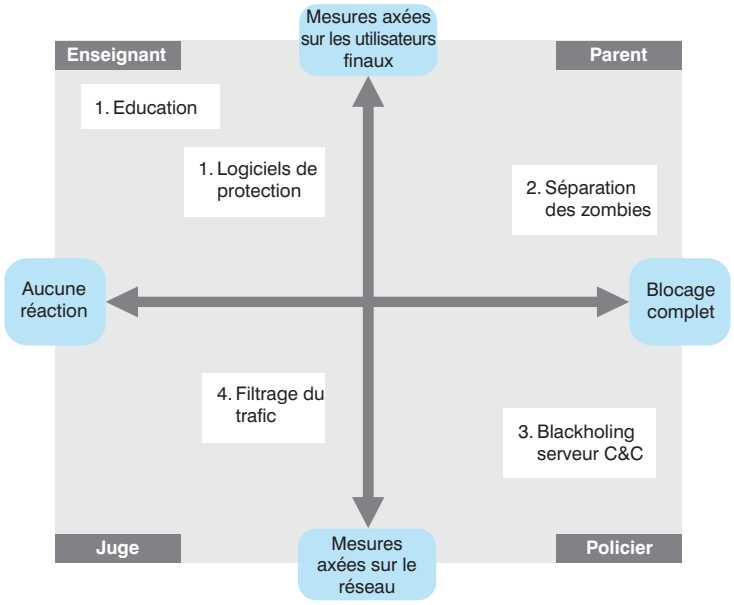
Blue Security avait développé et lancé la commercialisation d'un produit anti-spamming qui était réputé très efficace - et qui était, ironiquement, également basé lui-même sur un botnet[6]. Par la suite, Blue Security a été soumis au chantage par des spammeurs exigeant la cessation des activités. Suite au refus de Blue Security, une attaque DdS initiale a été lancée sur les serveurs de Blue Security qui y succombèrent. Les administrateurs redirigèrent alors l'entrée DNS vers TypePad, l'un des plus grands hébergeurs de blogs également utilisé par Blue Security. Des attaques DdS consécutives massives firent également succomber temporairement TypePad et Tucows, le fournisseur DNS de Blue Security – les deux étant de vastes et importants sites Web. Seule une riposte coordonnée par plusieurs opérateurs de réseaux et fournisseurs de services et destinée à protéger ces tierces parties permit de réduire les attaques atteignant des pointes de trafic de plus de 3 GBPS. Mais Blue Security resta hors ligne pendant plusieurs jours. Deux semaines après l'attaque initiale, Blue Security cessa ses activités anti-spamming.

*Le PDG de Blue Security, Eran Reshef, sur la lutte contre le spamming : « C'est quelque chose dont on devrait réellement laisser la décision aux gouvernements. Pour lutter contre les spammeurs, il faudrait réellement dépenser 100 millions de $. »**

**http://blogs.guardian.co.uk/technology/2006/05/17/spammers_kick_blue_frog_into_submission.html*

(6) Lorsque Blue Frog détectait un spammeur, toutes les machines utilisant Blue Frog envoyaient alors un e-mail au spammeur, constituant ainsi fondamentalement un botnet réalisant une petite attaque DdS envers le spammeur.

Illustration 42 : Matrice de la Confiance Numérique—réduction du botnet



(1) Blackholing utilisé seulement pour serveurs de contrôle, équipements attaqués par distribution de DdS, mais pas pour PC infectés

1. La majorité des FAI éduquent leurs utilisateurs et fournissent des logiciels de sécurité appropriés
   - Pour : Peut déjà prévenir une infection par des bots
   - Contre : La protection logicielle n'est pas sûre à 100%, connaissances techniques des utilisateurs nécessaires
2. Mise en oeuvre très limitée de la déconnexion des PC infectés de l'Internet dans un « jardin clos »
   - Pour : Le jardin muraillé minimise la vulgarisation des réseaux de bots
   - Contre : Problème de responsabilité avec faux positifs et suivi clientèle très intensif
3. Le blackholing correspond à la déconnexion des machines de l'Internet[1]
   - Pour : Très efficace, surtout pour les anciens botnets (ou pour réduire les attaques DdS)
   - Contre : Mesure extrême car tout le trafic vers cette machine est bloqué
4. Filtrage du trafic botnet – bien que très efficace, difficile à mettre en oeuvre
   - Pour : Minimise la menace d'autres activités avec peu de perturbations
   - Contre : Trafic botnet difficile à filtrer car très similaire au trafic normal

Une méthode plus centrée sur les utilisateurs mais interventionniste serait d'isoler les zombies, les ordinateurs individuels au sein d'un botnet. Ceci est une mesure de mitigation puissante mais difficile qui a été suggérée par le MAAWG (Groupe de travail contre les abus). Elle implique que les ordinateurs infectés soient séparés de l'Internet et placés dans un « jardin clôturé » contenant des mises à jour de sécurité et des possibilités de désinfection. Jusqu'ici, cette mesure a été implémentée dans un nombre de cas très limité seulement, par ex. dans de grands réseaux privés tels que certaines universités, en raison des problèmes potentiels de responsabilité juridique.

La mesure la plus efficace a toujours été le blackholing/la déconnexion du serveur de commande et de contrôle (C&C) du botnet. Par exemple, dès 2004, le FAI norvégien Telenor annihila un botnet de 10.000 zombies en arrêtant son serveur C&C. Mais les bot herders ont réagi à cela et utilisent désormais de plus en plus fréquemment des nouveaux types de botnets sans serveur central C&C.

Pour finir, une méthode également basée sur le réseau mais nettement moins interventionniste est le développement de techniques de filtrage du trafic à des fins de mitigation des botnets. Ici comme ailleurs, le filtrage a pour but de reconnaître le trafic botnet indésirable puis de bloquer les paquets IP respectifs de telle sorte qu'ils ne puissent pas atteindre leur destination. Le défi dans ce cas particulier est que le trafic botnet est très difficile à filtrer étant donné qu'il est très similaire au trafic Internet régulier. De nombreux FAI et opérateurs de réseaux utilisent actuellement une version simplifiée de cette méthode, en bloquant tout le trafic ressemblant au trafic typique des botnets – en prenant le risque de surbloquer les usages légitimes.

En outre, les FAI s'associent de plus en plus fréquemment à la mise en application des lois en surveillant l'activité du réseau et en communiquant les irrégularités. De cette manière, un vaste botnet a été supprimé aux Pays-Bas en 2005 lorsque le « fournisseur d'accès Internet XS4ALL notifia aux autorités une activité inhabituelle sur son réseau ». Le botnet se composait de 1,5 million de zombies, trois suspects furent inculpés.

ENSEIGNEMENTS CLÉS

Sept enseignements clés ressortent de la discussion :

- La nature des réseaux IP – c.-à-d. leur ouverture et leur neutralité – les a rendus très puissants mais les rend en outre facilement accessibles à des « intentions négatives » telles que les botnets.

- En raison de leur polyvalence dans des attaques potentielles, les botnets constituent une menace majeure envers l'intégrité du réseau et donc envers les opérateurs de réseaux, les fournisseurs de services, les entreprises et les consommateurs – l'activité botnet a en outre fréquemment des motivations politiques, comme en témoignent les exemples de l'Estonie et de Radio Free Europe.

- L'une des attaques les plus graves est l'attaque déni de service (DdS) utilisée pour couper certains sites ou pour soumettre des entreprises à un chantage – les botnets ont été responsable de toutes les attaques DdS majeures au cours des dernières années.

- La poursuite par la mise en application de lois joue un rôle important dans la lutte contre les activités des botnets – pour réussir, de telles poursuites nécessitent habituellement la participation d'autres parties prenantes, notamment celle des opérateurs de réseaux et des FAI.

- L'éducation est importante mais elle a un effet limité en raison de la complexité du sujet et de la difficulté même des consommateurs à détecter les infections.

- Les opérateurs de réseaux doivent réagir aux attaques graves de botnets par des mesures techniques de mitigation. Étant donné que la plupart des mesures sont complexes et qu'elles interfèrent avec le comportement des utilisateurs, les fournisseurs de réseaux doivent coopérer avec toutes les parties prenantes pour limiter les mesures nécessaires.

- L'isolation de bots dans des zones clôturées et la coopération avec les vendeurs de logiciels de désinfection des ordinateurs personnels s'avèrent être une solution efficace – mais les opérateurs de réseaux doivent trouver des moyens d'implémentation de ceux-ci d'une manière conviviale pour les utilisateurs (en minimisant l'entretien nécessaire par le client et en offrant des possibilités d'opt-out au cas par cas).

CAS 3 : BLOCAGE DU PHISHING

***Problème :** les mails de phishing ont pour but de voler l'identité de quelqu'un ou d'escroquer les consommateurs*

***Risque :** les consommateurs peuvent perdre des sommes d'argent considérables, par ex. en cas de vol des données de comptes bancaires en ligne ; l'authenticité des e-mails de phishing est souvent difficile à vérifier*

Le phishing a été présenté comme l'un des problèmes les plus critiques et connaissant une croissance extrêmement rapide dans le domaine de la protection de la vie privée et des données.

Aucun filtre anti-phishing n'est sûr à 100 %.

Étant donné qu'il s'agit d'un phénomène techniquement complexe, générer la prise de conscience et les connaissances nécessaires des consommateurs est une tâche difficile. Celle-ci est d'autant plus difficile que les e-mails et sites Web de phishing sont de plus en plus professionnels dans leur réalisation et difficiles à différencier des versions authentiques, même pour les experts spécialisés.

De ce fait, l'éducation peut seulement jouer un rôle accessoire dans la minimisation des dommages dus aux phishing. Mis à part l'intensification des poursuites des individus et des groupes responsables du phishing, le remède principal est de bloquer les attaques de phishing par le biais de méthodes techniques.

Les méthodes de blocage du phishing peuvent être décrites à l'aide d'une version adaptée du cadre de positionnement de la Confiance Numérique (Illustration 43) ; l'axe vertical différencie si l'usager doit se décider volontairement en faveur d'une solution (opt-in) ou si une protection est active tant qu'il n'enclenche pas la fonction opt-out, et l'axe horizontal différencie comment la solution peut être contournée.

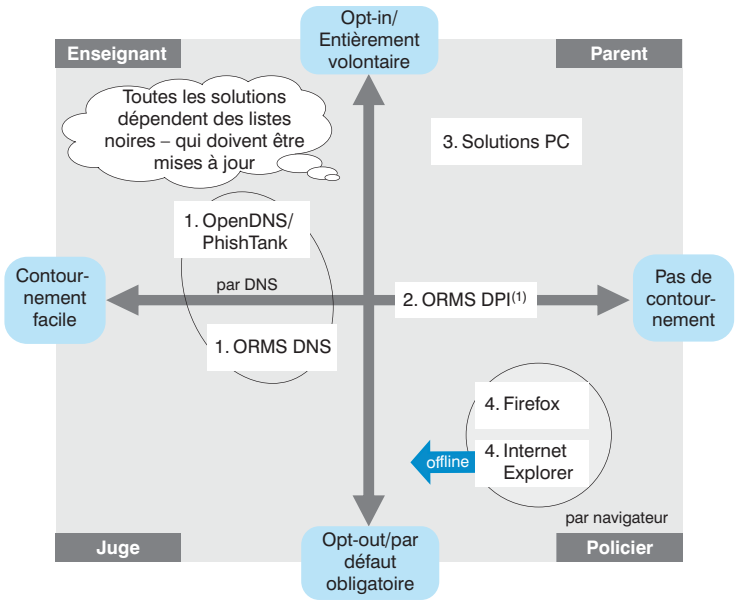
OpenDNS et PhishTank sont des exemples de procédures basées sur la communauté et visant à identifier les sites de phishing et à les inscrire sur une liste noire (Illustration 44). En raison de l'étendue de la communauté, les attaques de phishing sont détectées et contrôlées très rapidement, en moins de 12 heures.

Cette méthode concorde avec le filtrage DNS (système des noms de domaine) profitant du fait que des domaines spécifiques peuvent être bloqués individuellement. Elle peut être exécutée soit sur le serveur DNS du FAI, soit sur des serveurs de parties tierces. Le grand avantage de cette solution est qu'elle fonctionne sur toutes les applications, cela signifie qu'elle n'est pas limitée au trafic Web par l'intermédiaire d'un navigateur Internet mais qu'elle englobe par ex. également les e-mails. En même temps, cette méthode de blocage est seulement utile pour le phishing basé sur l'URL, ce qui la limite à environ 90 % de toutes les attaques de phishing (10 % des attaques sont basées sur l'adresse IP et n'utilisent pas les noms de domaines). Des barrières supplémentaires possibles sont par exemple le blocage basé sur le DNS qui peut nécessiter une configuration du système de l'utilisateur final en fonction de la solution ; dans le cas du blocage DNS basé sur le FAI, le surblocage peut être un problème substantiel étant donné que les possibilités d'accès de l'usager à un site donné peuvent être restreintes si celui-ci a été placé sur une liste noire par erreur.

La technologie est la clé du blocage anti-phishing – elle doit être appliquée à différents niveaux : réseau, ordinateur et navigateur

En second lieu, les FAI peuvent employer la vaste vérification de paquets (DPI) pour bloquer

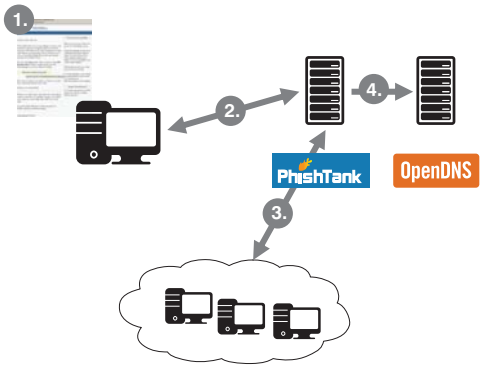
Illustration 43 : Matrice de la Confiance Numérique—blocage du phishing



(1) P.ex. solutions en relation avec l'addition de pub (Phorm)

1. Les solutions par DNS peuvent bloquer l'accès à des domaines spécifiques, sur le serveur DNS de l'ORMS ou sur des serveurs tiers
   - Pour : marche pour toutes les applications (pas seulement limité au navigateur mais aussi aux mails et autres)
   - Contre : seulement utile pour le phishing par URL
2. La solution de large vérification du paquet (DPI) sur le ORMS vérifie le contenu de tous les paquets et peut rediriger le trafic malveillant(1)
   - Pour : marche pour toutes les applications et de nombreuses attaques de phishing
   - Contre : problème du respect de la vie privée et contournement par cryptage
3. Les solutions de sécurité sur PC incluent normalement un filtrage du phishing
   - Pour : dépend de la solution, peut protéger toutes les applications
   - Contre : la solution doit être installée et configurée par l'utilisateur
4. Les navigateurs actuels peuvent comparer les URL avec les serveurs ou listes noires (heuristique également possible)
   - Pour : problèmes mineurs de respect de la vie privée (dépend de la mise en oeuvre)
   - Contre : pas de protection des autres applications, p. ex. mail ou anciennes versions du navigateur

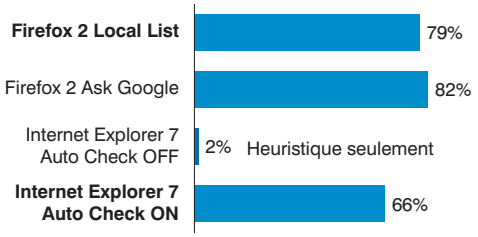
Illustration 44 : Synthèse du blocage du phishing



1. L'utilisateur reçoit un mail de phishing et se rend sur le site phishing – **L'utilisateur identifie l'attaque de phishing (par l'e-mail et le site Web)**
2. L'utilisateur soumet l'URL du site phishing à OpenDNS/PhishTank à titre de phishing potentiel
3. La communauté OpenDNS/PhishTank vérifie l'attaque de phishing
4. Le domaine est ajouté à la liste noire du PhishTank et bloqué dans OpenDNS
5. Toutes les tentatives d'accès au lien sont bloquées

Source : OpenDNS.com, PhishTank.com

Illustration 45 : Test d'efficacité du blocage de phishing par le navigateur (2006)



Gras : Mode par défaut
Source : Mozilla Foundation

les attaques de phishing. Les solutions DPI vérifient le contenu de chaque paquet se déplaçant sur le réseau et peuvent rediriger le trafic malveillant, c.-à-d. également le trafic vers des sites Web de phishing figurant sur des listes noires. Cette méthode fonctionne avec toutes les applications et donc avec la majorité des attaques de phishing. Néanmoins, elle provoque les inquiétudes habituelles associées à la DPI et concernant le respect de la vie privée : les consommateurs n'apprécient pas toujours le degré élevé de transparence de leurs données qui est généré dans ce cas par les fournisseurs de services, même si ces données sont sécurisées et ne sont pas utilisées à d'autres fins. L'utilisation de la DPI pour prévenir le phishing est très efficace et peut seulement être contourné par le trafic encryptant (qui est très rarement rencontré dans les attaques de phishing).

Troisièmement, l'ordinateur du consommateur peut être placé au centre des démarches : de nombreuses solutions actuelles de sécurité basée sur l'ordinateur contiennent un filtre anti-phishing – par exemple, les logiciels de sécurité de Norton, McAfee, Sophos ou autres, qui sont d'ailleurs fréquemment fournis aux consommateurs par le FAI ou l'opérateur de réseaux. De tels filtres peuvent être très efficaces étant donné qu'ils peuvent, suivant la solution choisie, protéger toutes les applications et assurer ainsi une protection forte contre le phishing. Un inconvénient de cette méthode est qu'elle nécessite une participation importante du consommateur, sachant que les solutions doivent être installées, configurées et actualisées. En particulier, la mise à jour régulière des listes noires locales est cruciale pour garantir de bonnes performances du filtre anti-phishing.

La mise à jour des listes noires est cruciale : seuls les sites de phishing y figurant peuvent être bloqués.

Enfin, le blocage du phishing peut être exécuté sur le navigateur. Les nouveaux navigateurs tels que l'Internet Explorer 7 et Firefox 2 peuvent vérifier les URL par rapport aux listes noires locales ou à celles du serveur afin d'identifier et d'agir contre les attaques de phishing. En outre, des actions heuristiques sont également possibles pour détecter les attaques de phishing (par ex. la détection d'attaques de phishing basées sur des modèles dans les URL habituellement utilisés pour le phishing ; mais cette méthode a un taux de réussite très faible de 2 % seulement). Un avantage de cette méthode est qu'elle ne provoque pas d'inquiétudes concernant le respect de la vie privée lorsque le blocage est effectué localement, c.-à-d. comme avec Firefox qui télécharge une liste de sites de phishing et qui effectue un contrôle automatique à l'aide de celle-ci. Une des limites de ceci est que le blocage basé sur le navigateur n'est d'aucune aide en cas d'attaque dans d'autres applications, par ex. les applications e-mail (ceci ne constitue qu'un problème mineur actuellement). En outre, cette méthode est vulnérable par rapport aux logiciels malveillants se trouvant dans l'ordinateur de l'utilisateur, par ex. un bot (voir chapitre III) désactivant la fonction ou manipulant les listes noires.

Le blocage de phishing basé sur le navigateur atteint un degré élevé d'efficacité lorsque des navigateurs nouveaux sont utilisés. Avec des navigateurs plus anciens tels que l'Internet Explorer 6, des fonctions externes doivent être utilisées (celles-ci utilisent normalement des listes noires similaires).

Dans les quatre méthodes, des listes noires sont nécessaires pour que le mécanisme de blocage puisse savoir ce qu'il doit bloquer. Ce qui figure sur la liste noire est donc crucial pour la réussite et l'acceptation du blocage de phishing : si une liste noire contient trop d'entrées, un surblocage a lieu, c.-à-d. des sites qui ne devraient pas être bloqués le sont (par ex. une page de log-in authentique d'une banque en ligne ayant été ajoutée à la liste noire par erreur) ; en revanche, si une liste noire ne contient pas toutes les entrées ou si elle n'est pas mise à jour suffisamment souvent, la protection n'est pas particulièrement utile et peut conduire à des problèmes de responsabilité pour le fournisseur de liste noire.

ENSEIGNEMENTS CLÉS

Cinq enseignements clés ressortent de la discussion :

- Étant donné que le phishing est difficile à comprendre pour le consommateur, il est probable que l'éducation soit d'une efficacité limitée – elle peut seulement jouer un rôle accessoire.

- Le blocage des attaques de phishing est l'un des remèdes centraux -- les diverses méthodes présentent toutes des avantages et des inconvénients concernant leur efficacité, leur exhaustivité (c.-à-d. quelles applications sont protégées), les problèmes de respect de la vie privée, la quantité d'actions requises du consommateur – tout ceci doit donc être soigneusement soupesé.

- L'aspect décisif au sein de toutes ces méthodes de blocage est la création et la gestion de listes noires indiquant les sites de phishing devant être bloqués. Aujourd'hui, différentes listes noires efficaces sont déjà disponibles (par ex. celles de Google, PhishTank) et utilisées dans les solutions modernes.

- Les solutions basées sur le navigateur sont les plus importantes aujourd'hui étant donné que ce sont elles qui permettent la plus grande interaction de l'utilisateur et qu'elles peuvent englober une éducation intégrée concernant la question en cas d'attaque. L'un des problèmes majeurs est que les navigateurs plus anciens ne contiennent pas de fonction de protection – il est nécessaire que l'industrie des logiciels coopère avec les FAI pour mettre sur le marché des versions plus modernes de navigateurs.

- Les méthodes les plus appropriées semblent être celles qui permettent aux utilisateurs (expérimentés) de désactiver ou de contourner au cas par cas le mécanisme de blocage (par ex. en cas de contenus figurant par erreur sur une liste noire), et qui permettent un plus grand respect de la vie privée des consommateurs (par ex. avec des listes noires locales).

CAS 4 : PUBLICITÉ CIBLÉE

Problème : les consommateurs produisent un grand nombre de données comportementales en utilisant l'Internet, et les entreprises souhaiteraient utiliser ces données pour une publicité plus ciblée

Risque/potentiel : les consommateurs sont préoccupés par le respect de leur vie privée mais les entreprises pourraient accroître considérablement la pertinence de la publicité (et donc les recettes)

Le Web 2.0 a entraîné l'essor de nombreux services basés sur les réseaux sociaux tels que Facebook ou MySpace. Un grand nombre de ces services ont établi de nouveaux records en termes d'abonnés et de croissance de l'usage – très fréquemment en raison du fait qu'ils sont offerts gratuitement aux consommateurs. Ceci fait cependant croître la pression exercée sur les fournisseurs, les incitant à monétiser ces services. Il est prévu que la publicité et notamment la publicité ciblée joueront un rôle central dans la monétisation des services Web 2.0 services – notre analyse de marché montre que la publicité sera le segment du monde numérique ayant la croissance la plus rapide (voir chapitre II). Les grands acteurs de l'Internet tels que Google ou Yahoo! ont déjà commencé à capitaliser la publicité – qui s'avère être leur principale source de revenus. En conséquence, l'industrie a récemment assisté à certains développements significatifs : Google a acquis DoubleClick, l'une des sociétés leaders de la publicité en ligne, pour 3,1 milliards de $ en avril 2007 ; AOL a racheté Tacoda, qui est spécialisé dans la publicité basée sur le comportement, en juillet 2007 ; et Yahoo a racheté Blue Lithium, qui est spécialisé dans la vente de bannières publicitaire basée sur la performance, en septembre 2007. De même, les fournisseurs de réseaux misent de manière accrue sur la publicité basée sur des modèles économiques pour réaliser leurs ambitions de croissance future.

Si elle est bien réalisée, la publicité ciblée peut amener une situation gagnant-gagnant pour les consommateurs et l'industrie : la publicité devient plus pertinente et, par là même, moins agaçante pour les consommateurs tandis que l'interpellation spécifique d'un public ciblé est plus rentable pour les annonceurs.

La logique économique est très simple : les groupes de consommateurs jeunes passent de plus en plus de temps sur le Web. Qui plus est, le Web

rend accessible aux annonceurs des informations supplémentaires sur le consommateur : quels sont ses centres d'intérêt ? Où vit-t-il/elle ? Une partie de ces informations est partagée ouvertement par le consommateur sur des plates-formes telles que Facebook, une autre partie des informations peut être obtenue en collectant les données sur le comportement en ligne.

La grande majorité voire l'intégralité de ces nouveaux modèles économiques requiert une collecte approfondie des données. Certaines implémentations récentes ont fait croître les inquiétudes relatives au respect de la vie privée. Aux États-Unis par exemple, la Commission fédérale du commerce (FTC) a invité à une conférence en novembre 2007 afin de débattre sur le thème de la « Publicité comportementale en ligne » en mettant en particulier l'accent sur les problèmes de respect de la vie privée, et a ensuite pris l'initiative de suggérer publiquement des « Principes de la publicité comportementale en ligne ».

Du point de vue de la Confiance Numérique, les facteurs et les principes liés à la publicité ciblée peuvent être reportés sur une version adaptée du cadre générique de positionnement de la Confiance Numérique (Illustration 46). L'axe horizontal différencie si la publicité ciblée est orientée sur le site Web/l'application (c.-à-d. les acteurs Internet tels que les réseaux sociaux) ou orientée sur le réseau (c.-à-d. les opérateurs câble ou FAI). L'axe vertical différencie le degré d'influence de l'utilisateur dans le consentement à l'utilisation de ces données dans une telle publicité, les possibilités allant d'une solution « opt-in » qui laisse entièrement la décision à l'utilisateur à une solution « aucun opt-out » qui utilise les données sans offrir à l'utilisateur la moindre possibilité de choix.

Il existe quatre exemples distincts illustrant comment implémenter la publicité ciblée. MySpace teste actuellement une solution déclarée spécifiquement opt-in. Facebook au contraire a lancé Beacon en 2007, une solution qui, à l'origine, a été implémentée sans le consentement des utilisateurs et qui était uniquement tournée vers une solution opt-out en réaction à un large débat public. Un exemple d'implémentation réussie de la publicité ciblée est Gmail : Google offre un service e-mail gratuit, mais analyse le contenu des e-mails des utilisateurs afin d'afficher des annonces ciblées sur l'interface. Ces annonces font partie intégrante de l'offre e-mail de Google : les utilisateurs doivent accepter le fait que la publicité affichée est choisie en fonction de leur correspondance e-mail – à en juger par le succès de Gmail, les utilisateurs ne semblent pas être trop inquiétés par cela. Gmail a cependant provoqué une vive controverse liée au respect de la vie privée lors du lancement en 2004. Les inquiétudes principales relatives à la vie privée concernaient le stockage illimité de données et le fait que les courriels adressés à des usagers de Gmail par des internautes non abonnés à Gmail étaient analysés sans leur consentement.

85 % des usagers rejettent l'idée de sites Web affichant des publicités basées sur les sites précédemment visités.

La solution MySpace HyperTargeting classifie les usagers sur la base de leurs centres d'intérêts énumérés sur le profil publié (plus de 100 catégories). Les annonceurs peuvent choisir des classifications de cibles pour leur campagne. Dans les tests initiaux, MySpace a réalisé une augmentation de 300 % des clics publicitaires (ce qui signifie qu'en comparaison avec la période précédente, 3 trois fois plus de clients ont cliqué sur un lien publicitaire) et 50 % de CPM supplémentaires. CPM signifie le coût pour mille impressions (coûts pour mille) – c'est le modèle standard utilisé pour payer la publicité sur la base du nombre de consommateurs ayant regardé une annonce. Bien que MySpace ait seulement effectué des tests jusqu'à présent, la discussion autour des problèmes de vie privée est déjà intense. Pourtant, utilisant la solution opt-in, MySpace a apparemment compris la nécessité de prendre activement en compte les préoccupations de ses usagers.

Plusieurs partenaires ont renoncé à leur participation après avoir réalisé que le Beacon de Facebook n'est pas une solution opt-in.

Par contre, le Beacon de Facebook était initialement mis en place pour tous les usagers, sans leur consentement préalable, lors du lancement en novembre 2007 avec 44 sites partenaires. Il intégrait Facebook aux sites partenaires, permettant l'échange de données détaillées et de profils tant que l'usager était connecté à Facebook. Conçu à l'origine pour permettre une consultation améliorée des histoires Facebook (« ton ami a regardé la vidéo xyz sur Joost »), il peut également être utilisé pour la publicité ciblée. D'importantes préoccupations concernant le respect de la vie privée sont apparues après le lancement, accompagnées de procès contre les sites participants. En réaction, Facebook s'est empressé d'introduire une option opt-out en décembre 2007.

Dans l'exemple Gmail, il est remarquable de constater que les inquiétudes potentielles sont abordées très ouvertement. Google a un texte détaillé sur son site Web expliquant de manière transparente que la publicité ciblée placée à côté d'e-mails a plus d'utilité et de valeur pour les usagers qu'une publicité non ciblée : « Google

pense que l'affichage de publicités pertinentes présente plus de valeur pour les usagers que l'affichage aléatoire de pop-ups ou de bannières publicitaires non ciblées ». Il est également probable que la solution Gmail soit vue d'un œil moins critique parce que les utilisateurs déclarent trouver la publicité utile et parce que les données ciblées sont utilisées de manière restrictive, uniquement pour des publicités destinées à l'usager respectif et uniquement au sein de l'application Gmail.

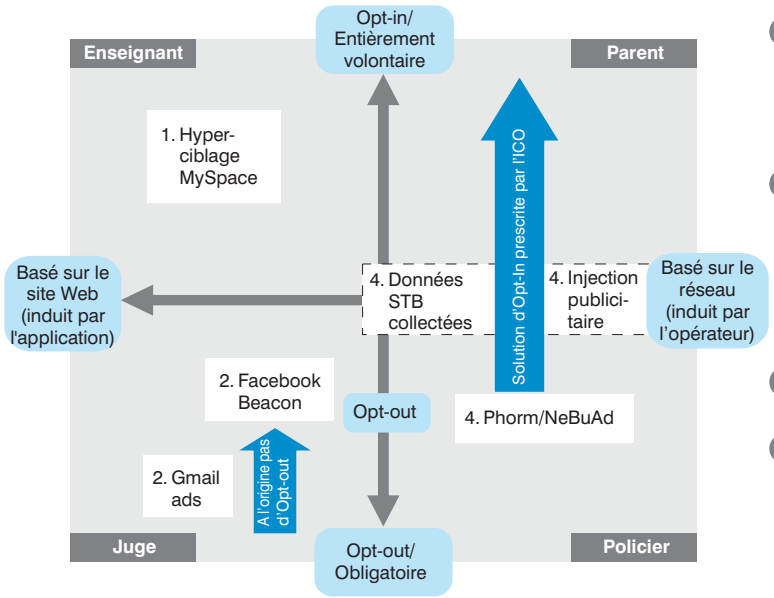
Phorm et NebuAd fournissent des solutions basées sur le réseau pour une publicité ciblée, ces solutions permettant d'analyser toutes les activités de navigation en ligne des utilisateurs, de telle sorte que les annonces affichées peuvent être ciblées de manière adéquate. Phorm sera prochainement testé par les principaux fournisseurs de réseaux, par exemple par BT et Virgin au Royaume-Uni. Phorm emploie la DPI pour analyser les activités de navigation sur le Web, considérant que tout le trafic est vérifié afin d'en dériver des profils.

Ces aptitudes hautement avancées de surveillance de l'Internet par la DPI – même d'un trafic anonyme – à des fins de publicité ciblée a intensifié l'attention et la surveillance des régulateurs à l'égard des risques majeurs relatifs à la vie privée. Bien sûr, l'extension de ces services sur certains marchés a provoqué une réaction violente des médias et la critique des usagers, notamment à cause de la façon dont les opérateurs de réseaux ont expérimenté ou voulu expérimenter ces technologies. Par exemple, BT a lancé un premier essai préliminaire de Phorm basé sur la publicité ciblée sans informer la base de clients concernés, ce qui a déclenché l'intervention de l'Office des commissaires de l'information (ICO) du Royaume-Uni qui a exigé que les clients choisis pour l'essai soient dûment informés de la technologie et qu'ils fournissent leur consentement en acceptant explicitement de participer, avec une possibilité de révocation à tout moment.

Charter Communications, le 4e plus grand opérateur câble des États-Unis, a stoppé au bout d'un mois son essai – annoncé – de publicité ciblée. Malgré la transparence appliquée et la présence d'une page de questions et réponses sur leur site Web, les usagers n'étaient pas convaincus des avantages communiqués (« une expérience de navigation améliorée »). D'autres inquiétudes concernaient l'usage de la DPI, considéré trop invasif. Des inquiétudes furent également soulevées quant à la garantie que les profits personnels ne seraient pas compromis. Enfin, la solution opt-out de Charter était considérée maladroite. Les usagers devaient remplir un formulaire et obtenaient alors un cookie spécial placé sur le navigateur. Le nettoyage des cookies ou le passage à un autre navigateur réactivaient cependant la publicité ciblée et imposaient de remplir une seconde fois le formulaire opt-out.

Au-delà de solutions telles que Phorm, une publicité ciblée basée sur le réseau peut également être réalisée par le biais du décodeur et sous forme d'injections publicitaires. Ceci permet aux

Illustration 46 : Matrice de la Confiance Numérique—publicité ciblée



(1) Les solutions actuelles sont axées sur le service publicitaire

1. L'hyperciblage de MySpace catégorise les utilisateurs en fonction de leurs centres d'intérêts listés et envoie des publicités en fonction de cette catégorisation
   – Les publicitaires peuvent choisir les catégories
   – En cours de test actuellement, mais soulève déjà des problèmes de respect de la vie privée
2. Facebook Beacon intègre Facebook dans d'autres sites (les activités sur d'autres sites sont transférées sur Facebook)
   – Devait permettre une plus grande vue des « Histoires Facebook », mais peut être utilisé pour une publicité ciblée
   – Gros problèmes de respect de la vie privée après son lancement, y compris actions en justice contre sites participants (Harris ./. Blockbuster)
3. Google Mail affiche des publicités en fonction du contenu des e-mails (reconnaissance automatisée du contenu)
4. Les solutions par ORMS analysent toutes les activités de navigation des utilisateurs d'Internet (publicité des sites participants ou injection de tous les sites[1])
   – Problème de respect de la vie privée puisque tout le trafic est vérifié pour en tirer des profils
   – Une tentative de BT sans le consentement des utilisateurs a fait que l'ICO du RU a demandé à Phorm de mettre en place des modèles de consentement préalable de l'internaute (opt-in) afin de se conformer à la législation britannique

fonctions de type communauté Web de pénétrer sur la plate-forme de télévision numérique (indices de popularité groupés) et permet la promotion croisée sur platesformes de même qu'une publicité mieux ciblée, étant donné que l'interface STB peut par ex. être utilisée pour afficher des annonces publicitaires interactives, par ex. pour promouvoir les offres de vidéo à la demande (VoD) basées sur les habitudes télévisuelles (« vous avez regardé 10 documentaires sur la vie sauvage en Afrique, souhaiteriez-vous télécharger un documentaire sur les lions ? »). La méthode se servant du décodeur fonctionne sur la base d'une saisie des données liées au comportement de « zapping » et aux programmes télévisés regardés.

ENSEIGNEMENTS CLÉS

Six enseignements clés ressortent de la discussion :

- La publicité ciblée connaît un essor manifeste favorisé par un ensemble de facteurs centraux : l'usage du haut débit comme phénomène de masse, la prolifération des technologies hautement avancées de surveillance Internet, la nécessité générale de nouveaux modèles économiques pour les acteurs de l'Internet et les fournisseurs de réseaux en vue de monétiser les nouveaux services et les nouvelles plates-formes du Web 2.0.

- Pour les fournisseurs de services Internet comme pour les fournisseurs de réseaux, la publicité ciblée sera la clé du financement des services de nouvelle génération et des innovations visant notamment à monétiser un grand nombre de services et d'applications du Web 2.0 – elle peut avoir une valeur accrue pour le consommateur si elle est convenablement réalisée (par ex. Gmail).

- En raison du grand nombre de données accessoirement générées par les sites de réseaux sociaux, ceux-ci se lancent avec entrain dans la publicité ciblée ; les fournisseurs de réseaux commencent seulement à considérer ces opportunités.

- Les mouvements précoces vers la publicité ciblée basée sur des technologies telles que la DPI ont attiré une forte attention du public et des médias, de même qu'ils ont soulevé de fortes inquiétudes relatives à la vie privée et provoqué le rejet dans de nombreux cas.

- Pour obtenir l'acceptation générale des usagers, il sera nécessaire de dépasser la simple observation des lois de protection des données et de la vie privée. Un élément clé est la transparence vis-à-vis des usagers au sujet du développement souhaité de la publicité ciblée. Il sera également crucial de faire clairement comprendre la valeur accrue d'une publicité ciblée pour le consommateur, c.-à-d. de convaincre les usagers de « ce qu'elle leur rapporte ».

- En ce qui concerne l'implémentation réelle par les opérateurs de réseaux, il est d'ores et déjà clair que les pratiques non transparentes pourraient mener à des obligations d'opt-in imposées par les régulateurs. Les outils opt-out faciles à utiliser et soutenus par une communication transparente aux usagers pourront cependant obtenir l'acceptation voulue, notamment en étant associés à un véritable service (gratuit ?) à valeur ajoutée, comme le montre le cas Gmail.

CAS 5 : BLOCAGE DES CONTENUS DE PORNOGRAPHIE ENFANTINE

Problème : bloquer l'accès aux sites Web montrant des contenus de pornographie enfantine (plusieurs milliers de sites)

Risque : le risque réel d'accéder involontairement à des contenus de pornographie enfantine est faible, mais il est possible de trouver de tels sites en les recherchant ; impact grave sur la vie des victimes

Les contenus de pornographie enfantine sont légalement interdits dans la majorité des pays du monde (avec cependant des différences dans la définition des termes « enfants » ou « mineurs », entre 14 et 18 ans dans la majorité des pays). Cependant, des milliers de sites Internet proposent encore ces types de contenus.

*Aux États-Unis, plus de 1.500 individus sont appréhendés chaque année pour possession de contenus de pornographie enfantine liés à l'Internet. La majorité d'entre eux possède plusieurs centaines d'images montrant des enfants âgés de 6 à 12 ans.**

La lutte contre les contenus de pornographie enfantine met l'accent sur la poursuite des personnes responsables de l'existence même de contenus de pornographie enfantine : utilisateurs/consommateurs de contenus de pornographie enfantine d'une part, fournisseurs de tels matériaux d'autre part. La poursuite des individus ou des entreprises contribuant à cela est la tâche exclusive des organes d'application des lois, qui sont susceptibles de requérir l'assistance d'autres parties prenantes (par ex. les fournisseurs de réseaux) si cela est jugé nécessaire et si les lois applicables le permettent. De fait, les gouvernements intensifient leurs activités dans ce domaine : très récemment en mai 2008, le Sénat américain a débloqué des fonds à hauteur d'1 milliard de $ sur les huit prochaines années pour lutter largement contre les contenus de pornographie enfantine.

** Centre national contre la disparition et l'exploitation des enfants*

La législation actuelle ne couvre pas l'ensemble des nouveaux problèmes liés à l'Internet et relatifs à des contenus d'abus sexuels.

D'un autre côté, la prévention des accès involontaires à des contenus de pornographie enfantine par les usagers d'Internet est une tâche incombant essentiellement aux fournisseurs de réseaux. Mais ceci est également plus difficile qu'il n'en paraît au premier abord, étant donné qu'il s'agit là d'une question à multiples facettes et vraiment controversée : un tel blocage fait de l'institution responsable la proie des critiques contre la censure et ravive la question des responsabilités juridiques ; en outre, un blocage imperméable est techniquement difficile sachant que les diverses techniques de blocage disponibles peuvent toutes être contournées.

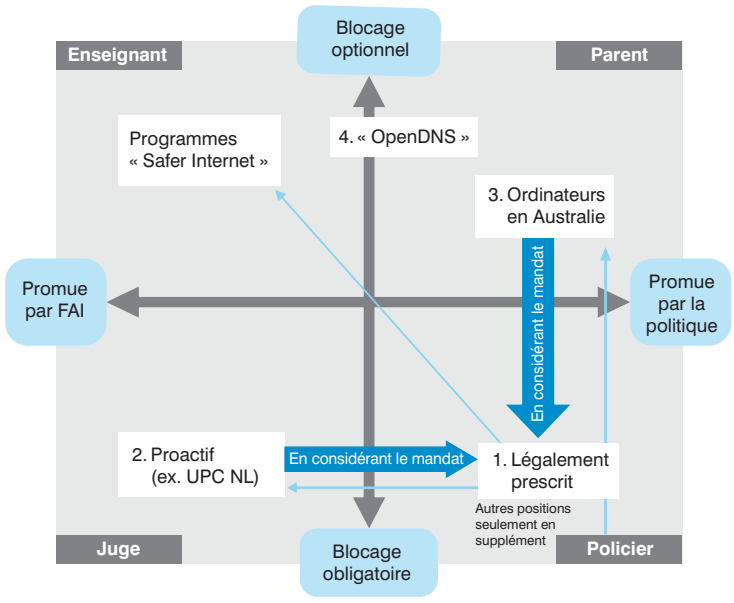
Un aspect problématique est le fait que les contenus de pornographie enfantine doivent être définis pour pouvoir être criminalisés et bloqués : la frontière entre la pornographie et l'art s'est déjà avérée être parfois floue. En outre, il est nécessaire que les critères de définition soient applicables : il est difficile voire impossible de déterminer si une jeune personne montrée dans un contexte pornographique doit être protégée ou non (c.-à-d. la question, dans la majorité des pays, de fixer une limite d'âge précise). De plus, les images créées ou modifiées à l'aide de logiciels de manipulation d'images constituent un problème (légal) différent qui n'était pas encore pertinent à l'époque où la majorité des lois ont été créées.

Les méthodes de blocage des contenus de pornographie enfantine peuvent être discutées en se référant à une version adaptée du cadre de positionnement de la Confiance Numérique ; l'axe vertical différencie si le blocage est optionnel (c.-à-d. laissé au jugement du consommateur), auto-imposé (c.-à-d. déterminé par l'opérateur de réseaux) ou obligatoire, et l'axe horizontal différencie qui, des opérateurs de réseaux ou des régulateurs, doit être la force agissante derrière cette activité.

Jusqu'ici, la méthode prédominante – au-delà du blocage de sites requis par la loi – est le filtrage auto-imposé des contenus de pornographie enfantine sur la base de listes de sites légalement interdits établies, entretenues et vérifiées par des tiers indépendants. Les FAI hésitent généralement à filtrer en se fondant sur le principe qu'en tant que « simples tuyaux », il n'est pas de leur rôle d'interférer avec les libertés de l'Internet. Qui plus est, ils désirent éviter les responsabilités juridiques leur incombant au cas où des contenus légaux seraient accidentellement bloqués. Si le filtrage est implémenté, volontairement ou par la force, des contrôles judiciaires indépendants sont alors nécessaires afin de déterminer que les contenus à filtrer sont véritablement illégaux au sein des juridictions compétentes.

Un exemple éminent de FAI prenant des initiatives proactives est le cas de l'initiative de filtrage des contenus de pornographie enfantine par UPC aux Pays-Bas au début de l'année 2007. UPC coopère avec le ministère néerlandais de la justice et la police néerlandaise qui établissent des listes noires sur lesquelles figurent plus de 3.000 sites Web contenant du matériel de

Illustration 47 : Matrice de la Confiance Numérique—blocage de la pornographie enfantine



1. Positions standard des FAI: ne bloquer le contenu que si prescrit par la législation
   - Pour : donne une protection de base
   - Contre : pas de protection supplémentaire possible
2. Les FAI proactifs développent des programmes de blocage sans y être contraints par la législation
   - Pour : prévient l'accès non intentionnel/aléatoire
   - Contre : pente dangereuse vers la censure si les listes noires sont utilisées par des tiers à des fins autres que celles initialement prévues
3. Le gouvernement australien a développé une solution sur l'ordinateur familial pour les parents
   - Pour : protection possible pour tous les citoyens
   - Contre : requiert des connaissances pour l'installation et la configuration
4. Des solutions de type OpenDNS sont induites par l'industrie et permettent aux utilisateurs de choisir les catégories à bloquer
   - Pour : FAI non responsable du contenu sélectionné
   - Contre : pas de niveau de protection uniforme – dépend de l'action individuelle & des préférences

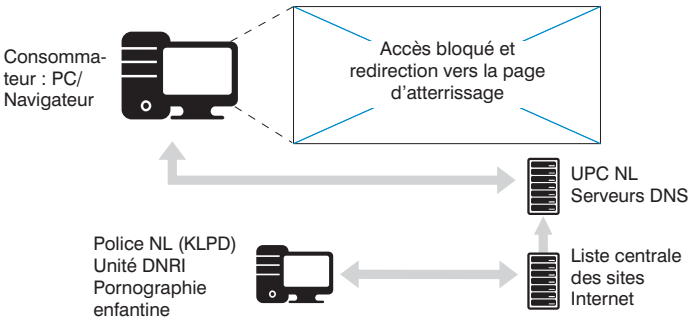
pornographie enfantine, et complique l'accès à ces sites en affichant une page intermédiaire énonçant que « vous êtes en train d'essayer d'accéder à un site Web figurant sur une liste noire ». Plusieurs milliers de fois par mois, cette solution a pu permettre de prévenir l'accès involontaire à des sites montrant des contenus de pornographie enfantine.

Les utilisateurs technophiles (même les enfants) peuvent facilement contourner la plupart des filtres présents sur les ordinateurs.

La réaction du public face à cette implémentation a été très positive. Dans un sondage consacré à cela, 95 % des consommateurs ont déclaré être en faveur de listes noires répertoriant les contenus de pornographie enfantine, et 94 % en faveur d'un filtrage par les opérateurs de réseaux des sites Web à contenus globalement indésirables. Ce dernier chiffre paraît très élevé, mais il est peut-être influencé par le fait que la question a été posée dans le contexte direct des contenus de pornographie enfantine et non dans le cadre d'un débat neutre. De plus, la majorité (63 %) des articles de presse sur l'activité de filtrage fut positive. En dépit de cela, des inquiétudes furent soulevées par le Parlement néerlandais au sujet de l'efficacité du filtrage DNS comme au sujet du fait que tous les FAI n'implémentent pas un filtrage. Le Parlement appela le gouvernement à examiner la faisabilité d'une obligation de filtrage (sous des formes potentiellement plus intrusives) à imposer aux FAI néerlandais.

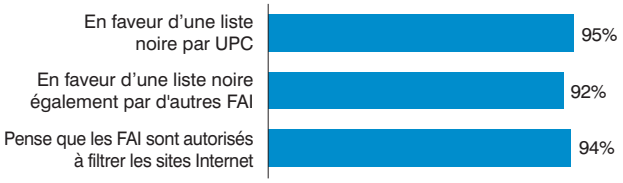
Le grand avantage des initiatives volontaires menées par les FAI est qu'elles peuvent fournir une protection élargie si les institutions fortes s'associent pour pallier la lenteur ou l'incompétence en la matière dans le cadre du processus de légifération. Le problème, du point de vue des fournisseurs de réseaux et des FAI, est qu'ils se rendent vulnérables face aux requêtes demandant l'élargissement du filtrage à d'autres genres de contenus — une « pente glissante » vers la censure et les problèmes de responsabilité. Quelques exemples pour illustrer ceci : en juillet 2007, la police suédoise tenta d'élargir une liste de contenus de pornographie enfantine en y répertoriant également le plus grand traqueur BitTorrent du monde, le site The Pirate Bay. Au Danemark, la cour a ordonné l'élargissement d'une liste de contenus de pornographie enfantine basée sur DNS pour y inclure certains sites populaires de téléchargement de musique (le site russe AllofMP3.com et The Pirate Bay une fois encore), provoquant ainsi une propagation d'informations concernant les méthodes de contournement qui minèrent l'efficacité du filtre d'origine.

Illustration 48 : Blocage de la pornographie enfantine—mise en oeuvre technique



Note : Solution technique simplifiée
Source : UPC

Tableau 49 : Blocage de la pornographie enfantine—opinion publique



Source : Interviews NSS (n = 600)

Une autre méthode a été observée en Australie : depuis 2007, le gouvernement australien examine une méthode sur deux fronts selon laquelle, d'un côté, les FAI seraient contraints au filtrage. Jusqu'ici, cette partie du projet s'enlise quelque peu suite à un certain nombre d'échecs au cours des essais sur le terrain, où il apparut que les solutions de filtrage n'étaient pas applicables de manière évolutive aux grands FAI. De plus, il existe une importante controverse politique concernant le type et la qualité des contenus devant figurer sur la liste noire administrée par l'ACMA (Autorité australienne des communications et médias).

De l'autre côté, le gouvernement a développé NetAlert, un programme visant expressément à « protéger les familles australiennes en ligne » et incluant le blocage des contenus de pornographie enfantine. Il s'agit d'une solution de filtrage de contenus basée sur l'ordinateur et comparable à de multiples solutions commerciales. Cette méthode place le choix et la responsabilité des consommateurs au centre, mais elle exige également de leur part un certain niveau d'initiative et d'expertise pour son fonctionnement. Étant donné que de nombreux usagers ne sont pas extrêmement technophiles, cette solution est difficile à déployer (quelques centaines d'installations seulement après le lancement) et facile à contourner pour les usagers plus expérimentés. Pour comble, il fut

rapporté qu'un adolescent avait réussi à contourner ce filtre de 84 millions de dollars australiens en 30 minutes.

Comme l'exemple australien le montre, aucune méthode de filtrage ne fournit de solution sûre à 100 % contre le contournement délibéré. De plus, un rôle crucial, dans tous les cas de filtrage, est joué par la qualité des listes de contenus illégaux – c.-à-d. la manière dont elles sont établies, entretenues/actualisées et mises en application. La vitesse à laquelle un contenu illégal répertorié est retiré du net constitue un problème supplémentaire. Il est rapporté que, suivant les procédures « notifier et retirer », les sites de pornographie enfantine restent en ligne pendant une moyenne de 30 jours après avoir été signalés pour la première fois. Le défi, pour les lignes de permanence nationales, est d'obtenir une application internationale des lois (par Interpol ou Eurojust) afin d'agir rapidement pour le retrait des contenus par les fournisseurs d'hébergement une fois que les lignes de permanence leur ont notifié la présence d'un contenu illégal dans leur ressort. Selon la Fondation de surveillance de l'Internet du Royaume-Uni, 2 % des sites commerciaux de pornographie enfantine dans le monde étaient encore actifs un an après avoir été identifiés.

L'absence de solution sûre à 100 %, les différences dans la qualité des processus de listage et les différents standards de mise en application sont autant de facteurs devant être pris en compte lors de l'évaluation des proportions du filtrage mandaté basé sur les FAI.

Enfin, le blocage des contenus de pornographie enfantine peut entièrement miser sur la responsabilisation du consommateur. Un cas exemplaire de cette méthode est l'implémentation de OpenDNS[7]. OpenDNS est un serveur DNS gratuit qui permet aux utilisateurs de choisir des catégories de sites devant être bloqués sur une interface Web. Le serveur DNS redirige alors l'utilisateur vers une page intermédiaire si une tentative d'accéder au contenu bloqué a lieu. La responsabilisation du consommateur comporte de grands avantages : les consommateurs sont libres de choisir ce qu'ils veulent voir ou bloquer (hormis ce qui est légalement interdit, bien sûr) ; ainsi, la censure et les discussions relatives aux responsabilités légales disparaissent d'elles-mêmes. En outre, une solution simple basée sur le réseau minimise la quantité de connaissances nécessaires à l'usager et est facilement accessible pour le « consommateur standard ». Pour la solution DNS basée sur le serveur, seule une configuration très restreinte est nécessaire en comparaison à l'utilisation de serveurs proxy ou de systèmes présents sur le disque dur de l'ordinateur. Pour obtenir les résultats désirés

Le filtrage de contenus pour lutter contre les contenus de pornographie enfantine peut s'avérer être une pente glissante vers la censure pour les FAI et les opérateurs de réseaux.

Listes noires de pornographie enfantine et coopération des NGO

Au Royaume-Uni, les FAI ont introduit des filtrages basés sur l'URL qui sont actuellement disponibles chez 96 % des clients haut débit. La liste URL est fournie par la fondation britannique IWF (Internet Watch Foundation) et contient plusieurs milliers d'URL ainsi qu'une moyenne de 250-300 noms de domaines de sites Web commerciaux qui proposent à la vente des images et vidéos d'abus sexuels sur des enfants. Six personnes travaillent à la ligne de permanence de l'IWF, elles effectuent le rapport, l'évaluation et le traçage des contenus et s'occupent de la maintenance de la liste URL de l'IWF. L'IWF actualise la liste deux fois par jour et demande à ses FAI membres de mettre à jour leurs filtres en conséquence, au moins une fois toutes les 24 heures. L'IWF partage sa liste avec d'autres lignes de permanence (jusqu'ici avec les lignes de permanence danoise, australienne et coréenne) sur la base d'un accord stipulant que la liste doit être réexaminée pour assurer sa conformité avec les lois dans les juridictions respectives.

Aux États-Unis, Verizon, Sprint & Time Warner Cable, AT&T et AOL ont signé un accord en juin/juillet 2008 pour empêcher l'accès aux sites et groupes de news pratiquant le trafic d'images de pornographie enfantine. Les entreprises doivent vérifier un registre de sites explicites maintenu par le Centre contre la disparition et l'exploitation des enfants. L'ambition de cet accord est de rendre extrêmement difficile la découverte ou la dissémination des contenus en ligne tout en sachant bien que ceci ne peut pas éliminer entièrement l'accès, étant donné que certaines parties tierces vendent des souscriptions payantes per-mettant aux clients d'accéder aux groupes de news de manière privée, et empêchant même leurs FAI de suivre leurs activités. Une bibliothèque de quelques 11.400 images illégales a été constituée, laquelle permet aux enquêteurs de filtrer parmi des dizaines de milliers de fichiers en ligne en même temps. Le système est basé sur les « valeurs Hash » uniques des images – une sorte d'empreinte digitale numérique – pour identifier les images illégales de manière à pou-voir ensuite chercher la même image ailleurs sur le Web.

www.nystopchildporn.com, une initiative de l'Attorney Général de l'État de New York, Andrew Cuomo, fournit les détails des FAI ayant signé les accords pour éra-diquer l'accès à la pornographie enfantine par le biais des serveurs utilisés à celle-ci.

cependant, il est nécessaire de donner des outils adéquats et faciles à utiliser aux consommateurs et d'éduquer ceux-ci, de même qu'il est nécessaire de gérer de manière adéquate les registres de contenus devant être bloqués, dans l'idéal au niveau de l'industrie.

ENSEIGNEMENTS CLÉS

Huit enseignements clés ressortent de la discussion :

- Le blocage des contenus de pornographie enfantine est communément perçu comme étant moralement justifié et donc souhaitable – les opinions concernant le blocage d'autres contenus « indésirables » (par ex. les sites Web racistes ou les sites « poudrières ») ne sont pas aussi unanimes, notamment du point de vue de la liberté d'expression.

- L'élargissement des listes noires à d'autres contenus tels que les sites illégaux de musique, qui sont populaires et loin d'être communément dénoncés comme les contenus de pornographie enfantine, peut entraîner des retours de flamme étant donné qu'il incite à faire circuler des informations sur les méthodes de contournement des filtres.

- Une exécution parfaite est un véritable défi du point de vue technique comme du point de vue juridique, étant donné que les législations diffèrent dans la définition de ce qui constitue un contenu illégal de pornographie enfantine. Les traités internationaux visant à créer des bases légales communes – comme la Convention du Conseil de l'Europe en 2007 sur la protection des enfants contre l'exploitation sexuelle et les abus sexuels – n'ont pas été mis en application dans tous les pays membres.

- Une méthode concertée sur le plan international pour la mise en application des lois est nécessaire pour accélérer le retrait des sites répertoriés sur les listes noires.

- Les attentes concernant l'efficacité du filtrage doivent être gérées. Aucun filtre n'est efficace à 100 %. Le filtrage basé sur le réseau est une simple contribution dans la prévention des accès involontaires aux contenus de pornographie enfantine. Ceci est un aspect important dans la discussion relative aux proportions d'un filtrage imposé par la loi.

- L'engagement en faveur du blocage des contenus de pornographie enfantine déclenche de vives controverses au sujet du risque de censure, des responsabilités et des différences entre les pays.

- Deux remèdes principaux en ressortent pour les opérateurs de réseaux et les FAI :

– Dans les pays où il n'existe aucun processus de listage adéquat et indépendant : responsabiliser le consommateur (c.-à-d. encourager largement les solutions de type Open DNS) et éduquer le consommateur au sujet des fonctionnalités et des possibilités de ces solutions ;

– Dans les pays où il existe un listage établi par une partie tierce : l'industrie doit décider volontairement du degré de filtrage à appliquer. En commençant par la forme la moins intrusive d'intervention, un premier pas pourrait être le filtrage basé sur le DNS, ou le passage au niveau supérieur avec le filtrage basé sur l'URL - uniquement s'il existe des listes adéquates et légalement vérifiées.

- Afin d'éviter les élargissements du filtrage au-delà de l'objectif initial qui est de lutter contre les contenus de pornographie enfantine, les institutions établissant les listes devraient être et rester indépendantes des autorités de justice ou de la police. La Fondation de surveillance de l'Internet du Royaume-Uni est un bon exemple de ce type d'organisations.

CAS 6 : ÉDUCATION SUR LES RÉSEAUX SOCIAUX ET L'INTERNET

Problème : les enfants et les jeunes ne sont pas conscients des risques de l'interaction en ligne (par ex. sur les réseaux sociaux) : sollicitation, grooming, etc.

Risque : en raison du fort anonymat de l'Internet, les risques sont plus élevés que dans la vie réelle (la majorité des enfants sait qu'il ne faut pas parler aux étrangers dans la rue ; mais qui est un étranger sur Internet ?)

Au-delà du blocage des contenus de pornographie enfantine (et, le cas échéant, d'autres contenus pernicieux et indésirables), il existe une deuxième manière déterminante de protéger les mineurs : les éduquer au sujet des opportunités et des menaces de l'Internet de telle sorte que les mineurs puissent eux-mêmes contribuer à leur protection.

Les acteurs de l'Internet disposent de plusieurs moyens d'éducation des enfants et des parents.

L'interaction sociale rendue possible par l'Internet, parallèlement à sa croissance rapide, a déclenché des problèmes qui étaient largement inconnus auparavant : le harcèlement en ligne, le grooming et la sollicitation tout comme la publication insoucieuse de données.

(7) Note : OpenDNS est disponible sur http://www.opendns.com. Nous nous référons à OpenDNS à plusieurs reprises comme exemple dans ce document étant donné qu'il s'agit d'une solution gratuite pouvant être testée par tous les lecteurs de ce document.

Le fait de devoir y faire face sans être préparé est une tâche fréquemment trop ardue pour les parents et les écoles en tant que « protagonistes habituels de l'éducation ». Plus ils se préoccupent de comprendre le monde de l'Internet, plus les deux choses suivantes sont nécessaires :

1. Les parents et les écoles doivent être responsabilisées (ou se responsabiliser elles-mêmes) pour pouvoir assumer les attentes d'éducation leur incombant.

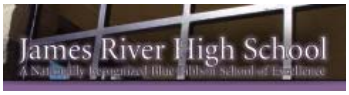
2. Les autres institutions – FAI, opérateurs de réseaux et entreprises Internet telles que les plates-formes de réseaux sociaux – doivent contribuer à l'effort global d'éducation.

Les méthodes d'une telle éducation peuvent être discutées en se référant sur une version adaptée du cadre de positionnement de la Confiance Numérique (Illustration 50). L'axe vertical différencie le degré d'activité – ici, la moitié inférieure est purement théorique étant donnée que l'option « aucune éducation » n'est pas viable. L'axe horizontal différencie l'appréciation individuelle d'une telle éducation, c.-à-d. la question de savoir si les méthodes font de l'éducation une offre optionnelle ou un devoir obligatoire.

Les réseaux sociaux rendent nécessaire un nouveau niveau d'éducation des usagers – tous les acteurs doivent prendre conscience de l'importance de ceci et fournir des solutions efficaces.

Premièrement, les sites de réseaux sociaux montrent un attachement clair à l'éducation des usagers, tel que le prouvent les exemples de Bebo, MySpace et Facebook. Ils tendent vers une démarche similaire en adoptant une position modérée dans la dimension obligatoire/optionnelle ; mais ils diffèrent notablement sur l'aspect proactif.

Bebo est une offre fortement orientée vers les mineurs qui, en conséquence, applique une approche clairement proactive en termes d'éducation des usagers. Par exemple, le site propose une vidéo éducatrice centrée sur les dangers des réseaux sociaux, dans un style amusant et divertissant conçu pour une compréhension réellement intuitive – spécifiquement ciblée sur les enfants. En outre, Bebo propose du matériel éducatif écrit pour les enseignants et les parents ; le développement de ce matériel a lieu en coopération avec un certain nombre d'ONG.

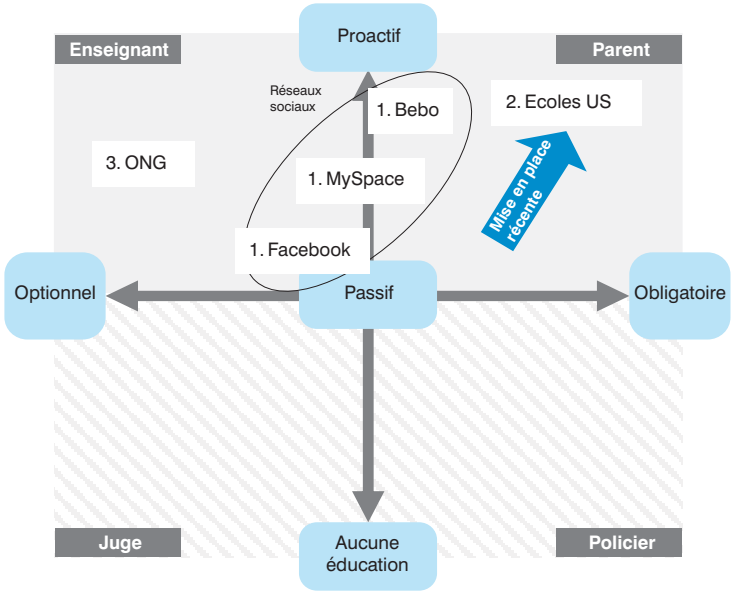


Facebook applique une méthode plus discrète d'éducation des usagers, vraisemblablement parce que ses groupes cibles se composent d'utilisateurs plus expérimentés et plus âgés. Le site propose à ses usagers un texte explicatif comportant cinq recommandations de sécurité ainsi que les questions fréquemment posées, mais également – spécifiquement pour les parents – des renseignements principalement axés sur les plaintes et procès.

Deuxièmement, les écoles aux États-Unis ont récemment lancé des cours spéciaux d'éducation à l'Internet et aux réseaux sociaux. La Virginie a déjà rendu obligatoires dans les lycées les enseignements sur la sécurité en ligne.

L'accent est mis sur les risques au sein des réseaux sociaux, notamment ceux de la persécution et de la sollicitation en ligne. Les cours se

Illustration 50 : Matrice de la Confiance Numérique—réseaux sociaux/l'éducation Internet



1. Les sites de réseaux sociaux éduquent leurs utilisateurs en termes de menaces et dangers du partage de données et d'un comportement crédule
   - Bebo très ciblé sur les mineurs et interactif, avec des paramètres très restrictifs par défaut
   - MySpace et Facebook moins ciblés sur les mineurs et moins restrictifs
2. Les écoles américaines lancent des cours spécifiques sur l'utilisation d'Internet et des réseaux sociaux
   - Concentration sur les risques des réseaux sociaux (harcèlement, sollicitation)
   - Cours obligatoire par exemple en Virginie
   - Supportés par les ONG, développement de supports pédagogiques (Web Wise Kids)
3. Les ONG telles que ConnectSafely cherchent à éduquer les enfants, parents et enseignants sur la façon d'utiliser Internet

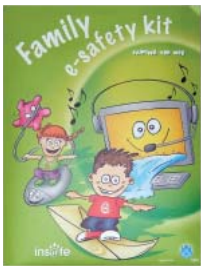
déroulent sur la base du matériel développé par l'ONG Web Wise Kids.

Troisièmement, un grand nombre d'ONG s'implique dans l'éducation sur les réseaux sociaux l'Internet, certaines d'entre elles mettant clairement l'accent sur les mineurs.

Reflétant la tendance omniprésente aux réseaux sociaux sur Internet, le thème essentiel de la sécurité dans la socialisation Internet a également son propre offre Web 2.0 : ConnectSafely est un forum ayant pour seul but « de discuter de la socialisation sécurisée sur le Web fixe et mobile ».

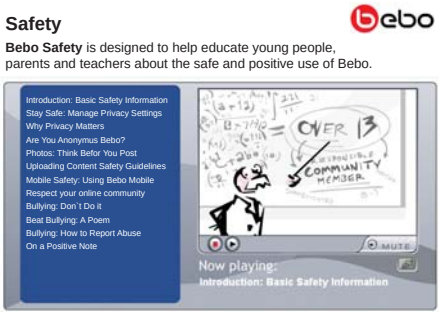
Web Wise Kids est une grande ONG basée aux États-Unis qui s'implique largement en faveur de la sécurité de l'Internet. Elle a développé plusieurs jeux numériques ciblés sur les enfants pour les éduquer au sujet du comportement général à adopter, des meilleures pratiques et des problèmes comme la sollicitation en ligne, les attaques de 'prédateurs' et le téléchargement illégal. Elle soutient également les écoles en fournissant individuellement du matériel de classe « hors ligne » et les adresses de diverses parties prenantes sur son site Web : de l'application de lois et des parents aux enseignants et aux mineurs eux-mêmes.

En Europe, Insafe est un réseau de noyaux nationaux qui coordonnent la prise de conscience de la sécurité sur Internet. Une activité exemplaire en est par exemple le kit Family e-safety, publié dans les pays européens au début de l'année 2008. Il traite les thèmes clés de la sécurité en ligne avec un design lui permettant d'être lu avec les enfants.



Malgré ces exemples positifs, il reste encore un long chemin à parcourir pour rattraper l'avance et la croissance rapide de l'usage d'Internet et des réseaux sociaux par les mineurs. Comme nous l'avons évoqué, il existe déjà un grand nombre d'initiatives positives. Mais il reste encore de l'espace pour une action mieux concertée réunissant diverses parties prenantes et permettant de partager les enseignements tirés, les meilleures pratiques et les formats éducatifs éprouvés – résultant en un effet limité des fonds investis globalement.

Illustration 51 : Formation du réseau social bebo



- Vidéo à destination des enfants distirbuée sur les réseaux sociaux, axée sur leurs dangers pour les enfants (vidéos style BD)
- Matériel pédagogique pour enseignants et parents
- Coopération avec plusieurs ONG pour le développement de matériel pédagogique

En particulier, l'introduction aux systèmes éducatifs formels en est seulement à ses débuts. Dans le même temps, les sondages révèlent que les parents considèrent les écoles comme la source primaire d'information sur la sécurité en ligne. Il est intéressant de constater que les « FAI ou sociétés de téléphonie» suivent immédiatement après. Bien que seulement 7 % mentionnent les sociétés de logiciels, l'intégration potentielle des mesures éducatives à l'interface primaire des utilisateurs (c.-à-d. les systèmes d'exploitation et les navigateurs) serait un pas logique permettant d'interpeller plus d'usagers de manière interactive.

Les parents attribuent essentiellement aux écoles la responsabilité de l'éducation à l'Internet.

ENSEIGNEMENTS CLÉS

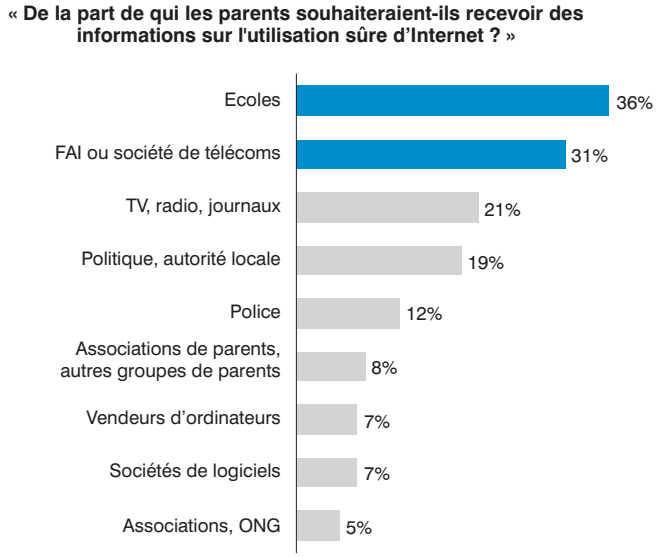
Six enseignements clés ressortent de la discussion :

- L'éducation des mineurs au sujet des opportunités et des menaces de l'Internet en général et des réseaux sociaux en particulier est de plus en plus importante.

- Les réseaux sociaux tentent d'éduquer leurs usagers, mais sur une base volontaire, à leur propre discrétion – il est donc nécessaire que la société surveille et complète les activités des réseaux sociaux.

- Les parents attendent des écoles et des FAI que ceux-ci jouent un rôle important dans l'éducation –ceci offre auxdites entités la précieuse opportunité d'accepter plus fortement encore ce rôle en intensifiant les activités déjà lancées.

Illustration 52 : Canaux d'information des parents (Royaume-Uni, 2006)



Source : Eurobarometer

• Les ONG ont déjà développé de larges activités dans ce domaine – ces activités doivent être consolidées dans le futur proche afin de permettre aux acteurs de joindre leurs forces et d'intensifier la coopération à plus large échelle, notamment avec les écoles.

• Une association entre les FAI et les ONG peut être une combinaison très utile permettant d'interpeller largement les masses avec une éducation en ligne et hors ligne.

• Toute éducation doit être ciblée par rapport au groupe (d'âge) spécifique sur le net, par ex. les membres de la génération 'née à l'ère du numérique' ont peu besoin dans leur adolescence d'une éducation technologique mais ont besoin d'apprendre les conséquences potentiellement négatives du partage de données et du partage de profils personnels en ligne ; les enfants plus jeunes ont besoin de conseils simples donnés de manière interactive ; les parents doivent apprendre le comportement en ligne réel de leurs enfants et doivent être capables de reconnaître à un stade précoce les symptômes d'une exposition à des dangers potentiels tels que le grooming ou la sollicitation.

CAS 7 : FILTRAGE DE CONTENUS SOUS COPYRIGHT

Problème : les contenus audio et vidéo piratés sont distribués en masse sur Internet et l'industrie des contenus doit faire face au défi urgent de trouver des modèles économiques pour le monde numérique

Risque : les opérateurs de réseaux sont contraints de restreindre l'accès aux offres de contenus ; ceci est potentiellement non conforme aux lois actuelles et limite l'expérience Internet des usagers

La prolifération des protocoles et des plates-formes de partage de fichiers, combinée aux vitesses accrues du haut débit dont peuvent disposer les utilisateurs finaux, a fait de la lutte contre la piraterie en ligne l'un des défis actuels les plus grands pour les régulateurs et les détenteurs de droits audiovisuels.

Depuis quelque temps, la priorité établie dans les politiques régulatrices sur la lutte contre la piraterie se tourne vers les fournisseurs de réseaux et les FAI, qui subissent une pression accrue les poussant à adopter un rôle plus proactif. Les mesures déployées que l'on peut observer comportent des solutions technologiques (par ex. la DPI et diverses formes de filtrage basé sur le réseau, les empreintes numériques chez les fournisseurs d'hébergement et les filigranes chez les fournisseurs de contenu) et des mesures non technologiques (telles que les notifications envoyées aux clients ayant été identifiés pour violation de droits), voir Cas 8.

Selon les réglementations de l'UE, les opérateurs de réseaux et les FAI, en tant que « simples tuyaux », sont exemptés de toute obligation générale de surveillance du trafic sur le réseau. Ils doivent uniquement s'engager à retirer les contenus illégaux qu'ils hébergent eux-mêmes après en avoir été notifiés. Ils refusent généralement de s'impliquer dans un filtrage « actif » de l'Internet visant à combattre les violations de copyright. La raison à cela est que la majorité des filtres technologiques pratiquent soit un surblocage – exposant les opérateurs de réseaux et les FAI à des responsabilités juridiques lorsque des contenus illégaux sont bloqués (dommage collatéral) ou lors de la restriction d'usages légitimes exemptés par la législation sur les copyrights ou sur la liberté d'information – ou un sous-blocage, parce que les personnes responsables de violations de copyright et les nouvelles technologies trouveront toujours des moyens de contournement. Trouver une solution volontaire ou même régulatrice est donc un défi. Il peut être très difficile (ou même impossible)

*Un fournisseur d'accès Internet renonçant volontairement à son immunité vis-à-vis des copyrights est comme un astronaute sur la Lune qui retirerait sa combinaison spatiale.**

*Tim Wu, professeur de droit, Columbia University

pour un opérateur de réseau ou FAI de distinguer une offre légale d'une offre illégale lorsque les deux utilisent exactement le même fichier. Il ne peut y avoir une méthode technologique unique pour tous et efficace à 100 %.

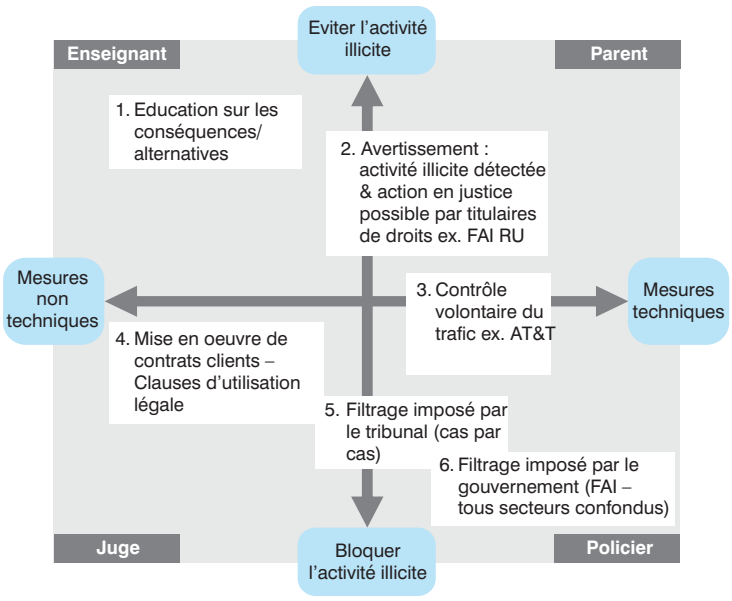
Par ailleurs, contrairement au débat sur le filtrage des contenus de pornographie enfantine, il n'existe aucun appui politique ou publique s'exprimant en faveur d'une certaine tolérance à l'égard de ces mesures potentiellement surbloquantes qui menacent de restreindre les libertés fondamentales de l'Internet pour défendre les intérêts commerciaux (même légitimes) d'une partie prenante spécifique. Lorsque, en janvier 2008, AT&T a annoncé son intention d'établir une surveillance proactive de tout son trafic pour détecter d'éventuelles violations des lois américaines sur la propriété intellectuelle, ceci a déclenché une réaction violente des consommateurs qui dénoncèrent des pratiques du type « Big Brother ». De même, le fait que AT&T prenne volontairement le risque de perdre son immunité par rapport aux responsabilités de copyright en adoptant un rôle actif dans la sélection des contenus transportés sur son réseau a été largement critiqué.

Ainsi, le filtrage obligatoire des contenus protégés par copyrights est, fréquemment, uniquement imposé par les tribunaux – au cas par cas.

En se référant à une version adaptée du cadre générique de positionnement de la Confiance Numérique, le filtrage peut être considéré comme une forme de réaction au partage illicite de fichiers qui peut être identifiée sur deux dimensions (Illustration 53). L'axe vertical différencie ce qui est actuellement entrepris pour combattre le partage illégal de fichiers, d'un côté en évitant que les usagers ne s'engagent dans une activité illégale, et de l'autre en bloquant l'activité illégale par le filtrage. L'axe horizontal va des mesures non techniques destinées à discipliner le comportement des usagers au déploiement de mesures techniques contre les personnes pratiquant le partage illégal de fichiers ou le téléchargement. Ici, le filtrage est le rôle du Juge lorsque, par exemple, un FAI individuel est contraint par un tribunal de bloquer l'accès à un site P2P particulier, ou le rôle du Policier lorsque tout un secteur de FAI est contraint d'installer des filtres par la législation.

The Pirate Bay (TPB) a été une « pomme de discorde » importante dans ce domaine au cours des dernières années. Il s'agit de l'un des sites de recherche torrents et traqueurs BitTorrent les plus connus et les plus grands. TPB a la réputation de distribuer un grand nombre de contenus protégés par copyrights (c.-à-d. piratés) tels que des films. Plusieurs FAI, par ex. le Danois Tele 2, ont été récemment contraints de bloquer TPB, tels que ceci est rapporté sur l'Illustration 54. Ce blocage forcé présente deux problèmes majeurs : la faisabilité technique et le soutien légal. Du côté technique, le réacheminement DNS peut être utilisé pour restreindre l'accès à TPB – mais les usagers trouveront des moyens de contourner ceci, ou, comme dans le cas du Danemark, TPB ajoutera simplement un autre nom de domaine indiquant la direction du site. En alternative, TPB pourrait être blackholé – mais ceci est une mesure très 'extrême' étant donné que, par exemple, tous les

Illustration 53 : Matrice de la Confiance Numérique—filtrage du contenu protégé par un droit d'auteur



1. Les FAI informent les clients des dommages causés par le partage illégal de fichiers et indiquent des alternatives légales
2. A partir des informations fournies par les titulaires de droits, les FAI avertissent les souscripteurs que leur compte Internet est utilisé à des fins de partage illégal de fichiers, pouvant entraîner une poursuite judiciaire de la part du détenteur des droits
3. Le contrôle volontaire du trafic par les FAI pour détecter la violation de droits d'auteur peut engendrer des allégations du type « big brother » par les clients ; éventuelle incertitude juridique pour les FAI
4. Les FAI peuvent choisir de mettre en place les stratégies « Utilisation légale » de manière plus stricte contre les contrevenants identifiés par les titulaires d'un droit d'auteur, p.ex. en envoyant des avertissements aux clients
5. Les FAI peuvent limiter/ bloquer l'accès à des sites spécifiques sur décision du tribunal
6. Les gouvernements peuvent adopter des lois intersectorielles imposant l'installation de filtres par tous les FAI

services à la même adresse IP seraient également coupés (mais il serait malgré tout encore possible de contourner ce blocage).

En mars 2008, la presse a rapporté que quatre géants de la musique avaient intenté un procès au FAI irlandais Eircom pour empêcher les usagers Internet de télécharger illégalement de la musique sur leur ordinateur – la première fois dans ce pays qu'un FAI était tenu responsable des actions de ses clients, au lieu de la poursuite des individus coupables des téléchargements illégaux. Ceci vient à la suite d'une décision dans un cas belge en juin 2007 dans lequel Scarlet, l'un des FAI leaders en Belgique, a été sommé d'installer une solution de filtrage à l'intérieur d'un délai de six mois. La décision avait alors alimenté une discussion intense portant sur la question de savoir si les opérateurs de réseaux peuvent être contraints de filtrer le trafic.

Enfin, le combat contre la piraterie par l'utilisation de technologies de filtrage high tech faisant partie de l'outillage de gestion des réseaux à la disposition des opérateurs de réseaux est récemment devenu un point central dans le débat sur la neutralité du net aux États-Unis. Les détenteurs de droits tels que MPAA et NBC ont appelé les opérateurs de réseaux à assumer un rôle proactif en employant des outils de gestion de la bande passante pour prévenir le transfert de contenus piratés. Ils argumentent que la neutralité du net doit promouvoir la protection de la propriété intellectuelle et non prévenir le développement de nouvelles technologies de filtrage et d'identification visant à détecter les contenus empiétant sur des copyrights. De l'autre côté, les groupes de défense des consommateurs comparent cette pratique à la censure.

ENSEIGNEMENTS CLÉS

Un certain nombre d'enseignements clés ressort de cette discussion :

- Les FAI hésitent généralement beaucoup à s'engager de manière proactive dans le filtrage du trafic Internet pour combattre la piraterie. Par nature, un rôle actif implique que les FAI interviennent dans les flux de trafic de leur réseau, minant ainsi leur statut de « simples tuyaux » qui garantit leur immunité vis-à-vis des responsabilités de copyright, celles-ci les exposants à leur tour à des revendications légales considérables.

- Le filtrage de contenus est difficile à mettre en œuvre, autant techniquement que légalement. Il aura très fréquemment pour conséquences soit un surblocage portant atteinte à un usage équitable, soit un sous-blocage des contenus empiétant sur des copyrights. Contrairement au filtrage des contenus de pornographie enfantine, il n'existe pas, à notre connaissance, de tierces parties indépendantes consacrées à l'établissement, la révision et l'actualisation de listes noires répertoriant les P2P illégaux. De plus, les technologies automatisées de filtrage de réseaux basées par ex. sur les empreintes peuvent être capables d'émettre une alerte rouge en présence de contenus protégés, mais elles

Illustration 54 : The Pirate Bay—évènements récents

- 1 million de torrents
- 12 millions de pairs (connexions actives simultanées)
- 2,5 millions d'utilisateurs enregistrés de sites

- Mai 2006 : Raid policier contre TPB
  - Confiscation des serveurs et autres équipements
  - Interrogation des fondateurs par la police, mais sans poursuite judiciaire
  - La MPAA aurait été la force principale de l'intervention
  - TBP de nouveau en ligne en juin 2006
- Juillet 2007 : La Suède veut mettre TPB sur la liste noire de pornographie enfantine
  - Aurait bloqué l'accès à partir de la Suède
  - Décision annulée – reproches de pornographie enfantine jamais prouvés
- Septembre 2007 : Des e-Mails de MediaDefender montrent que des sociétés de médias avaient engagé des pirates pour des attaques DdS contre TPB
- Janvier 2008 : Opérateurs TPB accusés de « promouvoir la violation des droits d'auteur par d'autres personnes »
- Février 2008 : La Tele2 danoise ordonne de déconnecter les clients de TPB
  - IFPI fait valoir que Tele2 viole le droit d'auteur en donnant accès à TPB
  - Appel de cette décision – viole la législation UE selon Tele2 car la copie est explicitement permise par la Directive UE Infosoc (Article 5.1)
  - Trafic du Danemark vers TPB en hausse de 12% en raison des débats publics
- Mars 2008 : FAI suédois en procès avec IFPI pour blocage de l'accès à TPB
  - Telia Sonera refuse parce qu'ils ne sont pas autorisés à mettre les clients sur écoute
  - Telia ne se sent pas responsable des agissements de ses clients
- Avril 2008 : TPB demande réparation à l'IFPI pour blocage de trafic par Tele2 DK

Sources : Article Actualités, The Pirate Bay, Wikipedia

ne sont pas en mesure de juger avec fiabilité si le contenu donné est réellement utilisé illégalement ou s'il fait partie d'une exemption autorisant un usage légitime. En outre, il faut aborder la question fondamentale de savoir si la protection des contenus sous copyright tombe sous la responsabilité des opérateurs de réseaux. Les coûts d'une telle action de l'opérateur se traduiraient alors par une augmentation des prix de ses propres offres.

• Dans les quelques cas où des opérateurs de réseaux ont annoncé l'intention de surveiller de manière proactive le trafic Internet, ces opérateurs se sont trouvés confrontés à de vives critiques des consommateurs portant sur le respect de la vie privée en raison de la nature intrusive des technologies de filtrage basé sur le réseau (par ex. la DPI ou d'autres formes de filtrage). Les entreprises risquent de se placer dans une situation de désavantage concurrentiel vis-à-vis des autres opérateurs qui ne filtrent pas de cette manière.

• Contrairement au débat sur les contenus de pornographie enfantine, le filtrage de contenus pour protéger les intérêts purement commerciaux d'une partie prenante spécifique tout en restreignant les libertés fondamentales de l'Internet ne rencontre pas un large soutien du public ni même des politiciens.

• Le filtrage basé sur le réseau a été critiqué parce qu'il enfreint les principes de neutralité du net en pratiquant une discrimination entre les différents genres de trafic et de services Internet. Ces technologies limiteraient l'usage légitime et l'expression légale, étoufferaient l'innovation et menaceraient la protection de la vie privée tout en n'abordant pas le problème sous-jacent. Parallèlement, les détenteurs de droits en appellent à la neutralité du net pour promouvoir la protection de la propriété intellectuelle et pour permettre aux technologies de filtrage et d'identification de contenus de se développer jusqu'à maturité.

• L'éducation des consommateurs joue également un rôle important, mais elle a ses limites étant donné que les usagers, en majorité, sont conscients de ce qu'ils font.

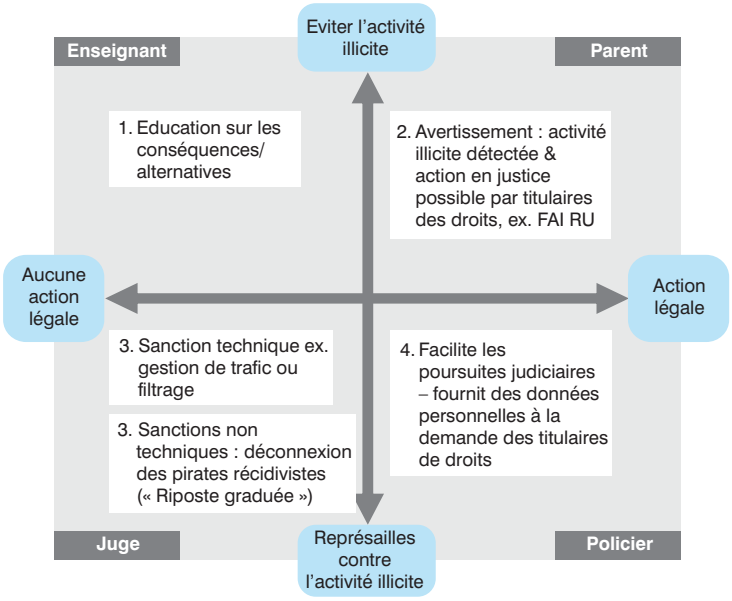
CAS 8 : ADOPTION DE LA « RIPOSTE GRADUÉE »

***Problème :** dans sa tentative de lutte contre la piraterie, l'industrie des divertissements désire introduire une règle de « riposte graduée » — les consommateurs empiétant sur des copyrights sont déconnectés de l'Internet au bout de trois attaques*

***Risque :** l'implémentation d'une règle de « riposte graduée » est susceptible de déconnecter des centaines de milliers de consommateurs de l'Internet, portant sérieusement atteinte aux droits personnels de ces individus et à la croissance de l'économie numérique*

À l'opposé des solutions technologiques de lutte contre les violations de copyright, il existe au niveau des opérateurs de réseaux et des FAI une série de mesures non techniques de mitigation qui sont activement débattues dans l'UE, aux États-

Illustration 55 : Matrice de la Confiance Numérique—« riposte graduée »



1. Les FAI informent les clients des dommages causés par le partage illégal de fichiers et indiquent des alternatives légales
2. A partir des informations fournies par les titulaires des droits, les FAI avertissent les souscripteurs que leur compte Internet est utilisé à des fins de partage illégal de fichiers, pouvant entraîner une poursuite judiciaire de la part du détenteur des droits
3. Le FAI est tenu (par co-régulation ou législation) de mettre en place des conditions contractuelles d'Utilisation Légale contre la violation du droit d'auteur (identifiée par les titulaires des droits) et de prendre directement des mesures :
   – Mise en place de mesures techniques telles que les filtres, la gestion du trafic
   – Mise en place de mesures non techniques : déconnexion (temporaire) de l'accès Internet – La « riposte graduée » est une combinaison de l'avertissement et de l'intervention active
4. Les FAI sont légalement tenus de fournir des données personnelles à certaines adresses IP à la demande des titulaires de droits – sans décision du tribunal – pour action civile
   – Requiert une vérification de compatibilité avec la législation sur la protection des données à caractère personnel

Note : Pour plus de détails sur le filtrage de contenu protégé par droit d'auteur, voir cas 7

Unis et au Japon. La plus hautement profilée parmi ces mesures est la règle baptisée « riposte graduée » (ou « trois attaques et vous êtes dehors »), qui a fait l'objet de campagnes actives menées par les détenteurs de droits sur les trois continents : son idée est de bannir réellement de l'Internet les consommateurs qui téléchargent massivement des contenus illégaux – une telle règle est un moyen de dissuasion puissant incitant les usagers à ne pas s'impliquer du tout dans des activités susceptibles de violer des copyrights.

En comparaison par rapport au blocage ciblé de services tels que The Pirate Bay qui servent principalement au partage (illégal) de fichiers ou par rapport au filtrage de contenus sous copyright, le risque de dépasser l'objectif initial est très élevé si l'on bannit complètement de l'Internet des usagers individuels « seulement » à cause d'une violation de copyright. La question de savoir si les intérêts commerciaux d'une industrie spécifique peuvent être un motif justifiant de couper complètement des individus de l'univers Internet est très discutable. De plus, il faut se demander si les opérateurs de réseaux ont le droit de jouer un tel rôle. Priver quelqu'un de l'accès à Internet est une pénalité grave qui devrait peut-être être seulement établie après que toutes les possibilités de procès en bonne et due forme sur la base des garanties légales ont été épuisées. Si les opérateurs de réseaux, en tant qu'acteurs privés, décident de couper quelqu'un en se basant sur les témoignages de détenteurs de droits, ils agissent alors en étant à la fois juge et partie. Le PDG de Carphone Warehouse, Charles Dunstone, déclare : « Notre position est très claire. Nous sommes le tuyau qui offre aux usagers l'accès à Internet. Nous ne contrôlons pas l'Internet, et nous ne contrôlons pas ce que font nos usagers sur Internet. Je ne vois aucune circonstance dans laquelle nous serions amenés à déconnecter volontairement un compte client sur la base d'une partie tierce alléguant un méfait. »

La règle « trois attaques et vous êtes dehors » fait partie d'un ensemble de réactions possibles à la détection d'un partage illicite de fichiers, tel qu'indiqué dans l'Illustration 55 et décrit dans le cas 7. La méthode de l'Enseignant lors de la détection du partage illicite de fichiers serait seulement d'informer l'utilisateur du dommage causé par le téléchargement ou le partage illégal – sans permission – de contenus protégés par copyright, et d'indiquer les alternatives, c.-à-d. les offres légales de contenus. En montant d'un cran dans le niveau d'intervention, la méthode du Parent impliquerait que l'opérateur de réseaux avertisse l'individu de manière proactive, sur la base de l'information des détenteurs des droits, qu'un ordinateur lié au compte Internet de l'individu est utilisé pour télécharger ou partager des contenus protégés. Il serait également expliqué que cette activité est équivalente à une violation de copyright pouvant mener à une action en justice intentée par les détenteurs des droits. Dans cette méthode, le fournisseur de réseaux pourrait également suggérer des logiciels de sécurité pour prévenir les téléchargements illégaux à partir du compte de l'utilisateur individuel. De cette manière, les opérateurs de réseaux peuvent minimiser les responsabilités et aider le consommateur à comprendre qu'il n'est pas anonyme à 100 % sur Internet.

Cette méthode est actuellement mise en œuvre par six FAI leaders au Royaume-Uni. Essayée tout d'abord par Virgin Media et la British Phonographic Industry (BPI) pour observer l'effet des lettres d'avertissement, ceci mena en juillet 2008 à une solution de co-régulation basée sur un Mémorandum de compréhension et rendue possible par le régulateur OFCOM. Ce Mémorandum de compréhension est destiné à fournir un cadre agréé d'action pour le combat contre l'usage illicite de la technologie P2P seulement – et non pas contre le problème de la piraterie commerciale. Il est signé par la BPI et MPAA représentant l'industrie des contenus, par Virgin Media, BSkyB, BT, Orange, Tiscali et Carphone Warehouse pour les FAI et par trois sections gouvernementales compétentes. Les signataires FAI acceptent de mettre en œuvre un essai sur 3 mois pour envoyer dans un premier temps des notifications à 1.000 souscripteurs par semaine identifiés par les détenteurs des droits musicaux. En outre, ils devront établir un Code de pratique – requérant l'approbation d'OFCOM – concernant les standards de la preuve ; actions contre les personnes prétendues coupables de violation et contre les personnes coupables de violations répétées ou criminelles ; indemnité en cas d'allégation incorrecte de partage de fichiers ; et routes d'appel pour les consommateurs. Jusqu'ici, les FAI du Royaume-Uni ne sont pas allés jusqu'à menacer les souscripteurs de déconnexion. Leurs lettres d'avertissement seront cependant accompagnées d'un avertissement écrit de la BPI qui menacera de déconnexion et de convocation devant les tribunaux ceux qui continuent à télécharger illégalement. Les remèdes contre les personnes récidivistes qui se montrent insensibles aux lettres d'avertissement sont encore débattus. Les solutions devant être discutées comprennent des mesures techniques telles que la gestion du trafic ou le filtrage, ainsi que le marquage de contenus pour faciliter leur identification.

La troisième méthode, le filtrage de sites

spécifiques de contenus empiétant sur le copyright ou de sites de partage de fichiers, a été présentée de manière plus détaillée dans le cas précédent.

La méthode la plus interventionniste, la déconnexion, est actuellement discutée et a déjà été introduite dans certains pays comme politique de « riposte graduée et vous êtes dehors ». Concrètement, l'action suivante a été très discutée (exemple de la France avec l'« Accord Olivennes » qui porte le nom de Denis Olivennes, le PDG du plus grand revendeur média français, la FNAC, et président de la Commission anti-piraterie qui a rédigé l'Accord et qui l'a présenté au président Sarkozy) : les FAI doivent envoyer des avertissements et mettre en œuvre des sanctions telles que requises par l'autorité anti-piraterie récemment établie, la HADOPI, qui évalue les notifications de violation émises par les détenteurs des droits et qui donne l'ordre aux FAI d'agir en conséquence. D'après ceci, les FAI doivent envoyer deux avertissements aux coupables présumés, le premier par e-mail. En cas de non-réponse et de récidive, un second avertissement est envoyé une semaine après par lettre recommandée. Au cas où il n'y aurait toujours pas de réponse et où les activités illégales continueraient, le compte d'accès est suspendu pendant 15 jours. Dans l'éventualité où il n'y aurait pas de réaction à cela et si la violation continue après la reprise du service, le compte est alors suspendu pendant (jusqu'à) un an.

D'une manière générale, une incertitude significative semble persister dans la question de savoir comment exactement la 'riposte graduée' doit être mise en œuvre – par exemple : visions divergentes sur la durée de déconnexion des usagers, manque de clarté concernant le processus de surveillance (la France est en train de débattre au sujet d'un registre des individus récidivistes à l'échelle de l'État) ; discussions quant à la responsabilité variable selon les pays (en particulier sur la question de savoir si les opérateurs de réseaux et les FAI doivent détecter toutes les violations ou s'ils doivent seulement réagir aux requêtes des titulaires des copyrights) ; problèmes de responsabilité (en cas de réclamations erronées concernant des récidivistes présumés) ; et, pour finir, la question de savoir qui doit payer une telle mise en œuvre.

Les pays ont adopté des positions variées par rapport à l'idée de la 'riposte graduée'. La France semble être la plus avancée dans la formulation de la méthode sous la forme d'un projet de loi devant être discuté devant l'Assemblée nationale à l'automne 2008. En France, la coopération des principaux FAI a été assurée en vue d'un accord garantissant en échange, entre autres, que de la musique serait offerte sans DRM pour le téléchargement légal. Le Royaume-Uni a semblé vouloir suivre l'exemple français et a activement examiné l'idée, au début de l'année 2008, au cas où les FAI et les détenteurs des droits ne parviendraient pas à un accord. Cependant, grâce au Mémorandum évoqué ci-dessus, la déconnexion des récidivistes n'a pas été mentionnée comme l'un des remèdes à discuter entre les parties signataires. La méthode au Royaume-Uni est également associée à un engagement des parties signataires les incitant à proposer des offres commerciales de contenus plus attractives (souscription, contenus à la demande, partage légal) comme alternatives au partage illicite de fichiers. Au Japon, les quatre principales associations de FAI se sont mises d'accord sur la mise en œuvre de la « riposte graduée » pour répondre à la pression du gouvernement et de l'industrie des contenus. En avril 2008, le Parlement Européen a rejeté la méthode de « riposte graduée » lorsqu'il a voté un rapport relatif à la promotion des industries européennes de la culture.

*Guy Bono, membre du Parlement Européen : « À ce sujet, je m'oppose fermement à la position de certains États membres dont les mesures répressives sont dictées par des industries ayant été incapables de modifier leurs modèles économiques pour faire face aux nécessités imposées par la société de l'information. La coupure de l'accès Internet est une mesure disproportionnée au regard des objectifs. Il s'agit d'une sanction aux effets puissants qui pourraient avoir de profondes répercussions dans une société où l'accès à Internet est un droit impératif en vue de l'intégration sociale. »**

Pour finir, la « riposte graduée » se présente comme l'une des mesures technologiques possibles basées sur les FAI et en cours de discussion dans le contexte de l'Accord commercial du G8 contre les contrefaçons (l'ACTA) que le G8 souhaite finaliser avant la fin de l'année 2008. L'ACTA concerne dans une large mesure l'actualisation des cadres légaux en vue de la prise en compte du P2P et du développement de l'Internet. Bien que ces procédures de négociation aient lieu à huis clos, certaines informations divulguées au sujet des propositions discutées semblent indiquer que la « riposte graduée » mais également le filtrage obligatoire par les FAI sont à l'ordre du jour.

*« Les six principaux fournisseurs d'accès britanniques ont signé un accord initié par le gouvernement pour réprimer le partage illégal de fichiers de musique. Les six fournisseurs — BT, Virgin Media, Orange, Tiscali, Sky et Carphone Warehouse — mettront en œuvre une série de mesures contre ceux pratiquant le partage de fichiers. Les FAI se déclarent peu disposés à imposer la méthode « riposte graduée ou vous êtes dehors » privilégiée par la BPI et consistant à couper les connexions haut débit des usagers. »***

Un aspect souvent négligé dans les discussions publiques sur les mérites de la « riposte graduée » est le dommage causé à l'économie numérique

** http://www.cableforum.co.uk/article/397/european-parliament-rejects-3-strikes-rule-is-vm-listening*

*** BBC News, 24 juillet 2008*

globale en conséquence de la déconnexion d'un nombre considérable d'usagers de l'Internet. Les implications de la « riposte graduée » nécessitent d'être comprises d'un point de vue plus holistique. Un calcul avec un niveau de sensibilité élevé, pour le Royaume-Uni par exemple, estime que la « riposte graduée » aura pour conséquence la déconnexion de 500.000 usagers et un manque à gagner de 180 millions d'€ pour les opérateurs de réseaux (Illustration 56). En comparaison, un aperçu sur l'industrie musicale permet d'évaluer une hausse des recettes de seulement 33 millions d'€ — ce manque à gagner total d'environ 150 millions d'€ représente probablement une part mineure des pertes pour les autres parties prenantes, par ex. par la réduction du volume du e commerce.

Outre le fait que les usagers sont alors déconnectés de de l'univers Internet, le dommage économique potentiel causé sur toute la chaîne de création de valeur de l'économie numérique fait également de la « riposte graduée » un concept osé au sein des discussions visant à trouver un remède proportionné et adéquat pour combattre la piraterie.

ENSEIGNEMENTS CLÉS

Quatre enseignements clés ressortent de la discussion :

- Par le régime de la « riposte graduée », les mesures de minimisation des violations de copyright sont amenées au niveau supérieur de l'interventionnisme, avec un danger substantiel de « dépassement de la cible » si les implications ne sont pas soupesées de manière équilibrée.

- Il paraît très douteux que les intérêts commerciaux d'une industrie particulière puissent être une raison incitant à couper complètement des individus de l'univers Internet – notamment au vu des coûts de mise en œuvre et d'opportunité impliqués pour les autres parties prenantes de l'économie numérique.

- Le débat public autour de la « riposte graduée » s'est concentré sur l'adéquation de l'idée elle-même – les préalables indispensables, en particulier les difficultés d'une détection correcte des violations de copyright et les implications au sens large, n'ont pas été suffisamment abordés.

- Selon les pays, les gouvernements et les opérateurs de réseaux ont agi différemment. Le Parlement Européen, dans sa résolution d'avril 2008 sur les « Industries de la culture en Europe », appelle les propriétaires de contenus à collaborer avec les opérateurs de réseaux et dénonce spécifiquement les mesures de criminalisation des consommateurs ne cherchant pas à tirer profit de leur acte comme n'étant pas la bonne solution dans le combat contre la piraterie numérique. En faisant fortement allusion à la méthode française, le Parlement incite à éviter les mesures « en conflit avec les libertés civiles et les droits de l'homme et avec les principes de proportionnalité, d'efficacité et de dissuasion, telles que la suspension de l'accès à Internet ».

2. LES POINTS À TRAITER PAR LES RÉGULATEURS

Les diverses activités gouvernementales et régulatrices au niveau de l'UE et des nations en relation avec la Confiance Numérique peuvent être regroupées en six points :

- Activités liées à la révision du cadre légal existant pour les fournisseurs d'infrastructures de communications et de services de communications électroniques.

- Activités liées à la réinterprétation des principes légaux tels que la Directive Européenne de protection des données

- Activités visant à faciliter la coopération entre les parties prenantes des différentes industries.

- Initiatives co-sponsorisées.

- Activités de légiférération au niveau de décision national.

- Activités destinées à mener la coordination.

2.1 ADAPTER LE CADRE LÉGAL ET LA POLITIQUE PUBLIQUE

En novembre 2007, la Commission Européenne a proposé une révision du cadre de régulation européen pour les fournisseurs d'infrastructures et de services de communications électroniques. La Commission envisage de légiférer à ce sujet avant la fin de l'année 2009.

Dans le contexte des menaces grandissantes telles que le spamming, les logiciels espions, les virus et les atta-ques de phishing, cette révision cherche à renforcer l'endurance des réseaux existants, tout en complétant la législation antérieure qui criminalise certaines activités. Concernant la Confiance Numérique, les objectifs de la révision visent principalement à :

- Augmenter la prise de conscience et les ressources des consommateurs, en particulier

vis-à-vis des brèches dans la sécurité des réseaux et au sujet de la vie privée en ligne. Par exemple, la Commission introduit le concept du rapport obligatoire des brèches de sécurité par les opérateurs de réseaux et les FAI.

• Améliorer l'expérience utilisateur par la promotion d'accès sans obstacles aux services numériques et en ligne en donnant aux autorités nationales de régulation la possibilité d'imposer des exigences minimales concernant la qualité du service.

En ce qui concerne la sécurité des réseaux et la vie privée des usagers, la révision propose spécifiquement que :

• Les consommateurs soient informés par les FAI si leurs données personnelles sont compromises en raison de brèches dans la sécurité du réseau.

• Les opérateurs et les régulateurs soient pourvus d'une plus grande responsabilité concernant la sécurité et l'intégrité des réseaux de communication électronique.

• Les pouvoirs de mise en application et d'implémentation des autorités compétentes soient renforcés, notamment dans la lutte contre le spamming.

• L'application des réglementations de l'UE relatives aux systèmes de collecte et d'identification des données en utilisant les réseaux de communications électroniques soit clarifiée.

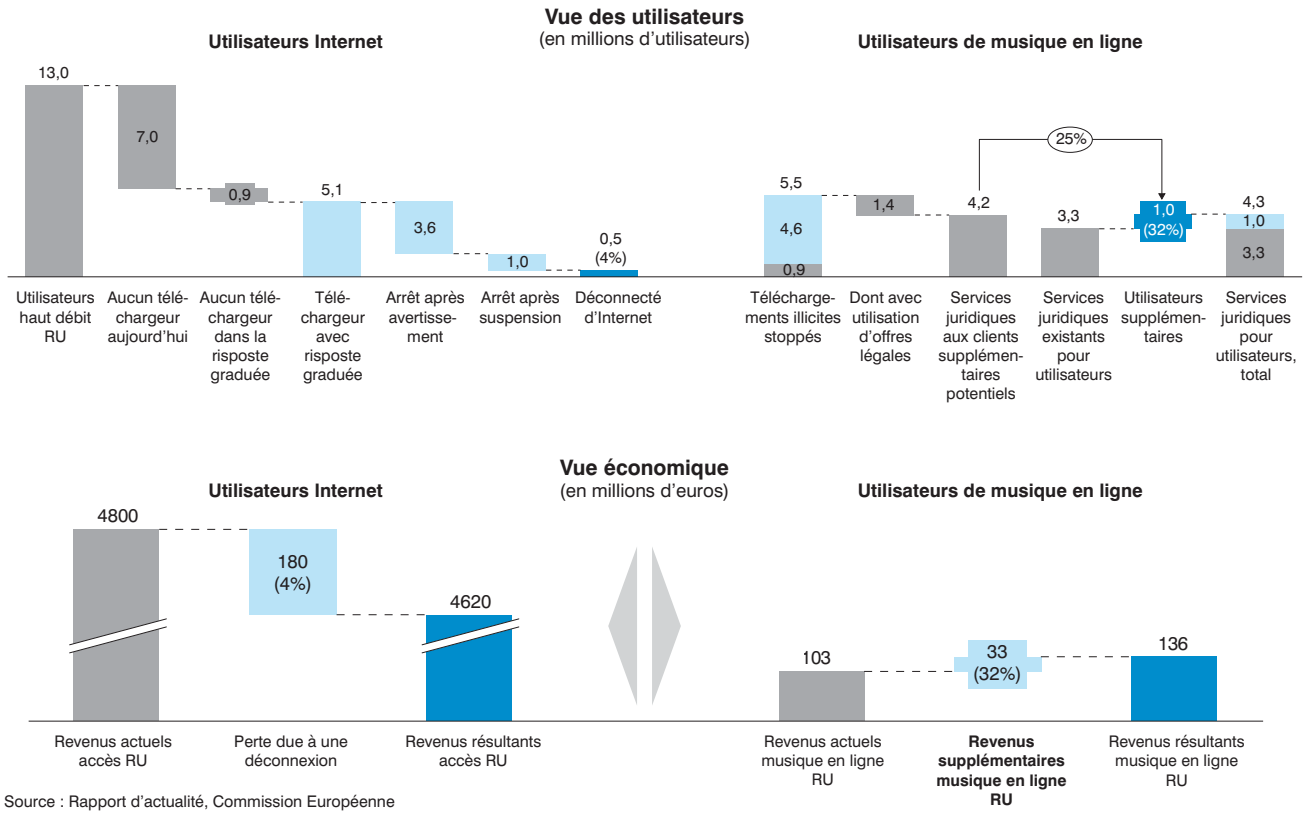
En ce qui concerne la garantie de l'accès des consommateurs à des services numériques et en ligne de haute qualité, la révision propose que :

• Les autorités nationales de régulation imposent des exigences minimales de qualité du service aux fournisseurs de réseaux de communications électroniques sur la base des standards développés au niveau européen.

Le but est de prévenir la dégradation du service et le ralentissement du trafic sur les réseaux à un niveau tel que la connectivité de base en serait sérieusement menacée. Conformément à l'Information Society Commissioner Reding, il restera cependant suffisamment de marge pour gérer et contrôler le trafic sur les réseaux afin d'optimiser le vécu en ligne des usagers, à condition que ceci soit fait de manière transparente, proportionnée et non discriminante.

La revue évoque également l'indépendance de l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) basée en Crète. Établie en 2004 au vu de la dépendance

Illustration 56 : Mise en oeuvre de la « riposte graduée » au Royaume-Uni—analyse de sensitivité



Source : Rapport d'actualité, Commission Européenne

constamment croissante vis-à-vis de l'ICT dans les processus commerciaux déterminants, l'ENISA cherche entre autres à stimuler la continuité des affaires en répertoriant les meilleures pratiques et les standards de mitigation des risques en développement afin de traiter les incidents perturbateurs sur les différentes infrastructures, tels que les attaques informatiques malveillantes ou la perte de données cruciales. Jusqu'à présent, l'ENISA a communiqué un certain nombre de recommandations, notamment concernant les problèmes de sécurité sur les réseaux sociaux en ligne, les botnets et les systèmes basés sur la réputa-tion. Reflétant les inquiétudes vis-à-vis de l'efficacité de l'ENISA à fournir un soutien opérationnel actif aux entreprises, la Commission a proposé de joindre l'ENISA à une nouvelle Autorité de Régulation européenne devant encore être établie. Étant donné que cette proposition d'un nouveau corps de régulation européen s'est avérée être très controversée, il n'est pas encore possible de savoir si l'ENISA sera effectivement regroupée à une autre entité ou restera indépendante. L'UE a néanmoins décidé que le mandat de l'ENISA sera renouvelé jusqu'en 2011, et que la nouvelle autorité de Régulation européenne – si une telle autorité vient à être établie – prendra alors la suite.

2.2 RÉINTERPRÉTER LES PRINCIPES LÉGAUX EXISTANTS

La réinterprétation des principes légaux est particulièrement importante dans le domaine de la protection des données et de la vie privée. Les développements actuels des services du Web 2.0 et des modèles économiques correspondants, par exemple le marketing comportemental et viral, les technologies de recherche et les réseaux sociaux, imposent la nécessité de faire respecter les principes fondamentaux de protection des données tels que la transparence, le consentement éclairé, la limitation des objectifs et le droit de rectification tels qu'ils sont fixés par la Directive Européenne de protection des données de 1995.

Le Groupe de travail Article 29 sur la protection des données révise constamment l'application des principes légaux établis par la Directive Européenne de protection des données aux nouveaux développements technologiques. Il a récemment adopté un nouvel avis concer-nant les problèmes de protection des données liés aux moteurs de recherche. Une conclusion clé de cet avis est que la Directive de protection des données s'applique généralement au traitement des données person-nelles par les moteurs de recherche. Les fournisseurs de moteurs de recherche doivent effacer ou rendre irrévocablement anonymes les données personnelles une fois qu'elles ne sont plus utilisées dans l'objectif spécifié et légitime pour lequel elles avaient été collectées, de même qu'ils doivent être capables de justifier à tout moment la rétention et la longévité des cookies em-ployés. Le consentement de l'usager doit être demandé pour toutes les relations croisées planifiées des données de l'usager comme pour les pratiques d'enrichissement des profils d'usagers. Les opt-out de l'éditeur de site Web doivent être respectés par les moteurs de recherche et les demandes d'actualisation des caches émises par les usagers doivent être immédiatement observées. La controverse a été ravivée notamment lorsqu'il fut connu que le Groupe de travail interprétait les adresses IP comme des données personnelles.

Les priorités du Groupe de travail à l'avenir visent à as-surer la protection des données en relation avec les nouvelles technologies en mettant l'accent, entre autres, sur les réseaux sociaux en ligne (en particulier pour les enfants et les adolescents), le profilage comportemental, le minage de données (en ligne et hors ligne) et la diffusion numérique.

2.3 FACILITER LA COOPÉRATION DES PARTIES PRENANTES

Étant donné les changements rapides dans la nature du marché, des modèles économiques et des technologies, la concertation des parties prenantes dans leurs efforts pour trouver des solutions rapides et efficaces est de plus en plus privilégiée dans les nouvelles approches législatives. Dans le domaine de la lutte contre la pira-terie des contenus sous copyright en ligne, la Commission entend établir une discussion entre les parties prenantes et une plateforme de coopération appelée « Plateforme sur les contenus en ligne ». Les consommateurs pourront largement s'exprimer sur cette plateforme.

Suite à la Communication de l'année 2008 sur les « Contenus créatifs en ligne au sein du marché unique », la Commission envisage par ailleurs l'encouragement de codes de conduite entre les fournisseurs d'accès/de services, les détenteurs de droits et les consommateurs afin de garantir une protection adéquate des œuvres protégées par un copyright et de resserrer la coopération dans la lutte contre la piraterie et le partage illicite de fichiers.

2.4 INITIATIVES SPONSORISÉES DE SOUTIEN À LA CONFIANCE NUMÉRIQUE

Au début de l'année 2008, la Commission a proposé un nouveau Programme pour un Internet plus Sûr afin d'améliorer la sécurité des enfants dans l'environne-ment en ligne. Ce programme vise à poursuivre et à développer le Programme

pour un Internet plus Sûr déjà lancé en 2005 et inclura également les services de communications plus récents de l'ère du Web 2.0 tels que les réseaux sociaux en ligne. Le nouveau programme proposé cofinancera des projets visant à :

- Fournir des points de contact nationaux permettant de signaler des contenus illégaux et pernicieux en ligne, en particulier les contenus d'abus aux enfants et le grooming.

- Encourager les initiatives autorégulatrices dans ce domaine et stimuler l'implication des enfants dans la création d'un environnement en ligne plus sûr.

- Augmenter la prise de conscience des enfants, des parents et des enseignants et soutenir les points de contact où ils peuvent obtenir des conseils leur indiquant comment rester en sécurité en ligne.

- Établir une base de connaissances concernant l'usage des nouvelles technologies et les risques liés en réunissant les chercheurs s'impliquant au niveau européen dans la sécurité des enfants en ligne.

Ces propositions comprennent des recommandations faites par les enfants eux-mêmes au cours d'un Forum de la Jeunesse Européenne ayant eu lieu lors de la Journée pour un Internet plus Sûr en février 2008. Le nouveau programme pour un Internet plus Sûr proposé (2009-2013) devrait en principe être adopté en 2009. Le cofinancement de nouveaux projets devrait commencer à partir de 2010.

Parmi les exemples de projets financés dans le cadre du Programme pour un Internet plus Sûr de 2005 se trouvent « Insafe » (pour permettre aux citoyens d'utiliser l'Internet de manière positive et sûre en favorisant le partage des meilleures pratiques, des informations et des ressources en interaction avec l'industrie, les écoles et les familles) et « INHOPE » (soutenant globalement les lignes de permanence Internet permettant de signaler des contenus illégaux tels que les contenus de pornographie enfantine ; voir la discussion sur la protection des mineurs au chapitre IV-1).

EXEMPLES TIRÉS DES DISCUSSIONS ACTUELLES SUR LA RÉGULATION

Japon : « Directives pour le contrôle du trafic », mai 2008

Au Japon, souvent évoqué comme l'un des marchés les plus avancés au monde en termes de vitesses de débit disponibles et d'extension des réseaux NGN, quatre associations de télécoms (Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Service Association, Japan Cable & Telecommunications Association) ont adopté en mai 2008 les « Directives pour le contrôle du trafic ». Selon un sondage du ministère de la communication japonais mené en novembre 2007, environ 40 % des FAI japonais ont implémenté des régulations des vitesses de débit.

Aiguillonnées par l'usage du partage de fichiers en P2P entraînant d'importantes augmentations du trafic, les directives sont destinées à réfréner les vitesses de débit pour les utilisateurs lourds. Le ministère de l'intérieur et des communications surveille les directives qui établissent des standards fondamentaux minimums pour le contrôle du trafic, en plus desquels chaque FAI établira et mettra en œuvre sa propre politique d'action. Les directives sont facultatives - les principes identifiés visent à élaborer un code de conduite qui serait considéré comme licite.

Les directives expriment qu'en principe, les FAI devraient faire face aux hausses du volume des commu-nications en améliorant leurs infrastructures. Une restriction des vitesses de communication devrait être seulement considérée dans certains cas exceptionnels. Par exemple, les fournisseurs peuvent restreindre les vitesses de communication des usagers lourds utilisant certains logiciels tels que les programmes P2P, ou de ceux essayant de télécharger vers des serveurs des quantités importantes de données au-delà d'un certain niveau, si leurs activités occupent une grande partie du réseau et entravent les communications d'autres usagers. Dans de tels cas cependant, les FAI doivent informer les usagers de ces mesures restrictives.

Les standards fondamentaux minimums concernent 1) l'envergure des informations nécessaires à l'application de l'accord contractuel ; 2) les exigences basiques requises pour effectuer le contrôle du trafic ; 3) l'action d'interprétation légale :

Celle-ci examine les bases d'une restriction de la bande passante pour certaines applications spécifiques ou pour certains utilisateurs spécifiques qui ont un impact disproportionné sur le réseau au détriment des usagers généraux.

Elle reconnaît qu'il existe des considérations de vie privée face à la DPI impliquée dans le contrôle des paquets (« confidentialité des communications ») et elle explique le potentiel de certaines exigences de « consentement de l'usager », mais elle présente aussi la base légale pour une exemption des exigences de vie privée et de consentement lorsqu'il existe un fondement « légalement justifiable » en faveur du contrôle de paquets.

Il existe des exemples dans lesquels cette pratique serait légalement justifiable – soit pour restreindre une application spécifique, soit pour restreindre un usager lourd spécifique – en mettant l'accent sur : (1) la légitimité de l'objectif ; (2) la nécessité de l'action ; et (3) la validité des moyens.

Ces exemples ne sont pas exhaustifs, il est reconnu que les pratiques seront amenées à évoluer ; en conséquence, les principes sont maintenus à un niveau élevé et visent essentiellement à assurer la stabilité de l'exploitation des réseaux.

Les directives recommandent une notification généralisée des pratiques de contrôle de paquets (c.-à-d. par opposition à l'exigence de consentement) et recommandent que cette notification soit claire pour les utilisateurs finaux, les utilisateurs intermédiaires et les autres FAI (c.-à-d. notamment les FAI en aval).

Royaume-Uni : 'Code de pratique volontaire : vitesses haut débit' de l'OFCOM, mai 2008

Au Royaume-Uni, les fournisseurs d'accès haut débit vantent aujourd'hui dans leurs publicités les débits « phares » pouvant être atteints sur leurs réseaux. En fonction de la technologie, de l'infrastructure et de l'environnement, ces hauts débits annoncés ne peuvent cependant pas être assumés pour certains consommateurs.

Le nouveau code exige des opérateurs de réseaux de fournir une estimation précise de la vitesse maximale pouvant être atteinte sur leurs lignes. En outre, le code demande une publication des pratiques de contrôle du trafic et des politiques en relation avec ceci (par ex. protocoles et applications touchés, limites d'usage équitable).

L'OFCOM examinera plus précisément les vitesses haut débit et reconnaît d'ores et déjà que les débits observés sur la durée sont susceptibles de s'écarter significativement des vitesses maximales. Dans le futur, l'annonce de vitesses moyennes pourrait donc également faire partie du code.

2.5 APPROCHES NATIONALES

Des divergences significatives dans les approches visant à combattre les menaces de la Confiance Numérique peuvent être observées selon les pays. Ceci est particulièrement manifeste dans la lutte contre la piraterie. L'approche de la France, avec l'Accord Olivennes visant à empêcher temporairement les consommateurs qui téléchargent illégalement d'accéder à Internet sur la base de la règle de « riposte graduée et vous êtes dehors », représente l'une des extrémités dans la dimension des approches nationales tandis que l'approche néerlandaise par exemple, avec la procédure « notifier et retirer » basée sur l'autorégulation des FAI, représente l'autre extrémité. L'approche française consistant à punir les personnes téléchargeant illicitement des contenus sur leur ordinateur est également l'inverse de ce qui est envisagé aux États-Unis, où ce sont les personnes téléchargeant vers les serveurs et non celles téléchargeant sur leur ordinateur qui sont ciblées sur la base des procédure « notifier et retirer ». Le téléchargement non autorisé d'œuvres protégées par copyright vers des serveurs est également illégal en France, mais l'accord ne fournit aucun support légal aux mesures technologiques destinées à appréhender les personnes téléchargeant vers les serveurs. Suivant l'Accord Olivennes, les FAI doivent mettre en œuvre l'identification des contenus (« empreintes digitales » et/ou filigranes) et la notification des problèmes à une autorité de régulation qui mène les actions contre les usagers concernés. Auparavant en janvier 2008, la Cour de Justice Européenne a statué, dans un cas impliquant la mise en application par les FAI, que les Directives de l'UE relatives à la protection des données et de la vie privée ne requièrent la mise en place d'aucune obligation imposant aux opérateurs de réseaux de révéler les données personnelles de personnes téléchargeant illégalement sur leur ordinateur, dans le cadre de procédures civiles permettant aux détenteurs de droits de poursuivre ces individus. Dans un tel cas, l'association espagnole des détenteurs de droits Promusicae avait demandé à un tribunal espagnol de contraindre Telefónica à fournir les identités et les adresses physiques des clients ayant utilisé le service P2P Kazaa pour le partage illégal de fichiers de musique. Comme avec la Résolution du Parlement Européen, le compromis difficile entre la protection des droits fondamentaux et la protection de la propriété (intellectuelle) a été établi en faveur de la sauvegarde des droits fondamentaux du citoyen, dans ce cas le droit à la vie privée.

La France, dans son rôle de présidente de l'UE pour le deuxième semestre 2008, a annoncé que ses objectifs politiques relatifs aux FAI n'incluraient aucune pression visant à instaurer une réplique exacte de l'Accord Olivennes au niveau européen. La présidence de la France vise plutôt à réunir autour d'une table toutes les parties prenantes afin d'encourager les négociations.

Enfin, il est utile de mentionner que la « riposte graduée » compte parmi les propositions faisant actuellement l'objet de discussions actives au niveau du G8. L'Accord commercial contre les contrefaçons (ACTA) que le G8 souhaite adopter avant la fin 2008 pourrait inclure la « riposte graduée » et le filtrage obligatoire par les FAI pour tenter de répondre aux actuels défis de l'Internet et du P2P, pour lutter contre la piraterie et imposer des sanctions criminelles correspondantes.

2.6 COORDINATION INTERNATIONALE

Suite aux attaques DdS contre l'Estonie (voir cas 6), le Sommet de l'OTAN à Bucarest s'est mis d'accord au début du mois d'avril 2008 sur une politique commune de cyber-défense et s'engagea à établir une nouvelle autorité ayant pour tâche primaire de coordonner les réactions « politiques et techniques » de l'OTAN aux attaques en ligne.

Mis à part un nouveau corps, une véritable approche commune européenne de cyber-défense nécessite également que chaque État membre établisse une structure nationale de prévention et de défense contre les attaques en ligne comme l'Équipe de préparation aux urgences informatiques des Etats-Unis (US-CERT), un partenariat entre le Département de Sécurité de la Patrie et les secteurs privé et publique. Créée en 2003 pour protéger les infrastructures Internet du pays, l'US-CERT coordonne la défense et les ripostes face aux attaques en ligne dans tout le pays. Actuellement, seuls quelques états européens possèdent de telles structures.

L'Information Society Commissioner Reding a annoncé qu'au début de l'année 2009, la Commission présentera une Communication sur la protection des infrastructures télécoms déterminantes. Celle-ci serait destinée à améliorer la préparation et les capacités de riposte au niveau européen en cas d'attaques en ligne. Le Commissaire a souligné l'importance des développements techniques sans oublier la nécessité d'une éducation accrue concernant les avantages et les risques de la société de l'information. Cette ligne paraît bénéficier d'un soutien fort de la part de l'industrie.

2.7 CONCLUSION

Les principaux fondements légaux pour gérer les défis de la Confiance Numérique semblent être largement en place, avec cependant cer-

taines nécessités de réinterprétation des concepts régulateurs existants afin de prendre en compte les nouvelles technologies et les réalités du marché, du marketing et des usages. La nature transfrontalière des menaces envers la Confiance Numérique rend particulièrement importantes la coopération internationale (judiciaire), une prise de conscience accrue de l'urgence de l'action et, pour les gouvernements et les autorités de mise en application, l'allocation de ressources appropriées visant l'établissement de structures efficaces de mitigation et de partenariat avec l'industrie. Au niveau de la politique et des organes de régulation, il semble y avoir une tendance au renforcement de la coopération entre les parties prenantes plutôt qu'à celui des activités législatives – de fait, ceci n'est pas seulement visible en Europe mais également aux États-Unis avec les mouvements récents de la FCC. Parallèlement, une révision continue de la proportionnalité des activités régulatrices est nécessaire, notamment dans le cas des approches fortement interventionnistes (telles que la « riposte graduée » ou le filtrage obligatoire) qui sont susceptibles d'empiéter sur les libertés fondamentales de l'Internet, les droits fondamentaux des consommateurs (par ex. à la vie privée) et d'ébranler les certitudes légales acquises des acteurs de l'industrie.

L'industrie a néanmoins l'opportunité d'intensifier ses responsabilités dans ce domaine ; un témoignage en sont les nombreuses activités d'éducation et de responsabilisation des consommateurs pour améliorer leur confiance dans l'usage des nouveaux services numériques et en ligne. En complément des initiatives de responsabilité d'entreprise menées par l'industrie - si cela en vient à une mise en application, une coopération accrue entre secteurs et avec les organes gouvernementaux et régulateurs est nécessaire pour fournir un fondement légal à même de soutenir chaque niveau d'intervention planifiée. Citons ici l'exemple des divers niveaux de filtrage et de blocage de contenus, où les opérateurs de réseaux voudront garantir que leurs responsabilités soient couvertes. Dans le domaine de la sécurité des réseaux également, des partenariats entre le publique et le privé pourront être nécessaires en tant que base de stratégies cohérentes et efficaces de mitigation pour garantir une collecte efficace des données souvent hautement sensibles et confidentielles.

Botnets militaires pour une guerre de l'information

En mai 2008, le Col. Charles W. Williamson III a proposé qu'Air Force bâtisse son propre réseau de zombies, afin de pouvoir lancer des attaques déni de service sur des ennemis étrangers. Il recommande qu'Air Force installe délibérément des bots sur ses ordinateurs non classifiés, de même que sur les machines du gouvernement civil.

Dans une première réaction, les autres officiers de la Marine proposèrent d'installer des bots même sur les systèmes de sécurité de l'information existants et de réutiliser les ordinateurs normalement destinés à être jetés, pour monter une « armée de bots ».

Les commentateurs civils de Wired considérèrent cela comme étant « l'idée la plus démente provenant de l'Armée depuis la bombe gay ». D'un autre côté, l'efficacité de larges attaques DdS ne peut pas être niée – comme cela a été vu récemment en Russie où des pirates informatiques ont fait succomber la majorité des sites Web russes de l'énergie nucléaire par une attaque DdS.

Source : Wired, Darkreading

V. ANALYSE DES RISQUES ET BÉNÉFICES : LA CONFIANCE NUMÉRIQUE EST RENTABLE

Tel que décrit dans les chapitres précédents, le thème global de la Confiance Numérique est un thème complexe. La Confiance Numérique comporte non seulement un facteur essentiel de bien-être (« je me sens bien, je suis en sécurité ») pour les consommateurs, mais également un important impact économique. Par exemple, la piraterie en ligne a aujourd'hui un impact économique de plusieurs milliards d'Euros en Europe. Dans chacun des domaines clés de la Confiance Numérique, il s'agit de gérer des compromis qui ont des impacts sociétaux et, pour la majorité d'entre eux, des impacts économiques. Par exemple, une protection très restrictive de la vie privée du consommateur est susceptible d'avoir un impact sur les nouveaux modèles économiques basés sur la publicité ciblée et individualisée – qui est un élément contribuant fortement aux 57 milliards d'€ du marché de la publicité en ligne en Europe en 2012. Il est important de réaliser qu'aujourd'hui déjà, de nombreux services en ligne utiles et novateurs – tels les planificateurs d'itinéraires ou les plans de villes – ne peuvent être offerts gratuitement à un public de masse que parce qu'ils sont financés par la publicité. Ces services seraient alors susceptibles d'être soumis à de fortes pressions, et de nouveaux services ne seraient pas réalisés.

Par ailleurs, les rôles et les responsabilités au sein de la Confiance Numérique entre toutes les parties prenantes sur la chaîne de valeur de l'économie numérique doivent être définies afin de garantir la réalisation d'une approche cohérente qui permette aussi bien la création de valeur pour l'industrie que la satisfaction des attentes des usagers par rapport aux prestations de l'industrie le long des quatre piliers de la Confiance Numérique. Ces rôles et responsabilités doivent refléter un partage équitable des charges et doivent être proportionnés aux rôles respectifs des diverses parties prenantes sur la chaîne de valeur. Les opérateurs de réseaux étant des acteurs essentiels de la croissance et aussi bien transporteurs que fournisseurs de services Internet et numériques sur leurs réseaux, il ne fait aucun doute qu'ils doivent continuer à jouer un rôle absolument central pour encourager la Confiance Numérique ; leur position commerciale essentielle de « tuyau » est placée devant un défi très fort en termes de valeur future qui sera largement générée par le commerce et les services à valeur ajoutée.

Par exemple, une règle telle que la « riposte graduée et vous êtes dehors » préconisée par les propriétaires de contenus et leurs associations requiert des fournisseurs de réseaux qu'ils assument un rôle dans la surveillance et le maintien en ordre de l'usage des contenus sous copyright sur leurs réseaux. Cette approche pourrait cependant mener à une perte directe globale d'environ 150 millions d'€ par an pour le Royaume-Uni dans les recettes de l'économie numérique – en plus des implications relatives à la vie privée des consommateurs.

Pour comprendre l'impact économique de la réussite ou de l'échec de la Confiance Numérique, nous avons mené une analyse visant à obtenir une vue holistique de l'économie numérique et de ses recettes en Europe, aujourd'hui et plus particulièrement à l'avenir, et à évaluer en chiffres concrets les effets d'une Confiance Numérique solide ou faible. Jusqu'à présent, plusieurs études et comptes-rendus ont montré et estimé l'impact des mesures individuelles dans le domaine de la Confiance Numérique, chacun d'entre eux partant de différentes suppositions et étant valable seulement pour des régions géographiques limitées. Pour notre appréciation, nous avons tiré profit de toutes ces données de départ et bâti un modèle holistique cohérent pour l'ensemble de l'Europe et pour toutes les mesures de la Confiance Numérique.

Cette analyse des risques et bénéfices procure une vue complète indiquant quels piliers de la Confiance Numérique ont le plus grand impact financier. Elle évalue l'impact sur les recettes de l'économie numérique européenne de deux scénarios alternatifs comparés à un cas de base. Concrètement, elle indique en détail à quel degré les pools de revenus de l'économie numérique sont mis en danger par les problèmes de Confiance Numérique, et elle fournit à cette occasion une vue des stimulations financières incitant l'industrie à concentrer son attention sur le développement de solutions favorisant la Confiance Numérique. Comprenant ceci, les gouvernements et les régulateurs peuvent ensuite soutenir les tentatives de l'industrie dans des domaines plus motivés par des intérêts sociétaux que par des intérêts financiers.

Le risque d'une Confiance Numérique qui ne fonctionne pas est élevé : une valeur de marché de 124 milliards d'€ jusqu'à 2012 – l'équivalent d'environ 1 % du PIB européen – pourrait être perdue.

Tel que décrit dans les chapitres précédents, le thème global de la Confiance Numérique est un thème complexe. La Confiance Numérique comporte non seulement un facteur essentiel de bien-être (« je me sens bien, je suis en sécurité ») pour les consommateurs, mais également un important impact

économique. Par exemple, la piraterie en ligne a aujourd'hui un impact économique de plusieurs milliards d'Euros en Europe. Dans chacun des domaines clés de la Confiance Numérique, il s'agit de gérer des compromis qui ont des impacts sociétaux et, pour la majorité d'entre eux, des impacts économiques. Par exemple, une protection très restrictive de la vie privée du consommateur est susceptible d'avoir un impact sur les nouveaux modèles économiques basés sur la publicité ciblée et individualisée – qui est un élément contribuant fortement aux 57 milliards d'€ du marché de la publicité en ligne en Europe en 2012. Il est important de réaliser qu'aujourd'hui déjà, de nombreux services en ligne utiles et novateurs – tels les planificateurs d'itinéraires ou les plans de villes – ne peuvent être offerts gratuitement à un public de masse que parce qu'ils sont financés par la publicité. Ces services seraient alors susceptibles d'être soumis à de fortes pressions, et de nouveaux services ne seraient pas réalisés.

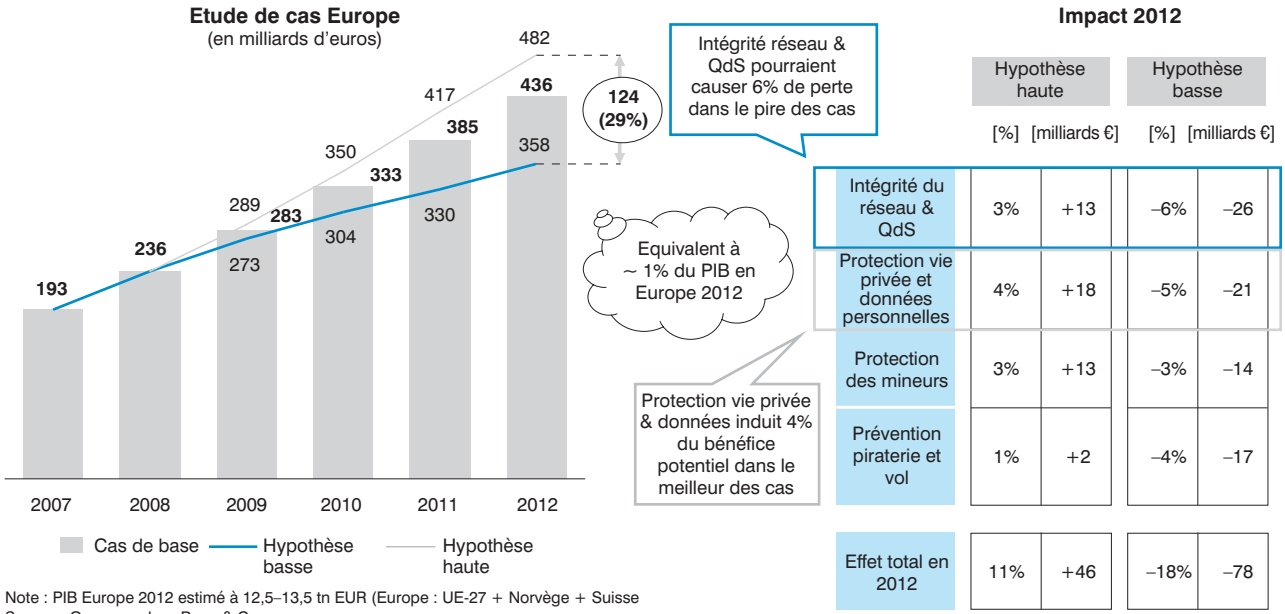
Par ailleurs, les rôles et les responsabilités au sein de la Confiance Numérique entre toutes les parties prenantes sur la chaîne de valeur de l'économie numérique doivent être définies afin de garantir la réalisation d'une approche cohérente qui permette aussi bien la création de valeur pour l'industrie que la satisfaction des attentes des usagers par rapport aux prestations de l'industrie le long des quatre piliers de la Confiance Numérique. Ces rôles et responsabilités doivent refléter un partage équitable des charges et doivent être proportionnés aux rôles respectifs des diverses parties prenantes sur la chaîne de valeur. Les opérateurs de réseaux étant des acteurs essentiels de la croissance et aussi bien transporteurs que fournisseurs de services Internet et numériques sur leurs réseaux, il ne fait aucun doute qu'ils doivent continuer à jouer un rôle absolument central pour encourager la Confiance Numérique ; leur position commerciale essentielle de « tuyau » est placée devant un défi très fort en termes de valeur future qui sera largement générée par le commerce et les services à valeur ajoutée.

La « protection de la vie privée et des données » et l'« intégrité du réseau et la qualité du service » ont l'impact économique le plus considérable.

Par exemple, une règle telle que la « riposte graduée et vous êtes dehors » préconisée par les propriétaires de contenus et leurs associations requiert des fournisseurs de réseaux qu'ils assument un rôle dans la surveillance et le maintien en ordre de l'usage des contenus sous copyright sur leurs réseaux. Cette approche pourrait cependant mener à une perte directe globale d'environ 150 millions d'€ par an pour le Royaume-Uni dans les recettes de l'économie numérique – en plus des implications relatives à la vie privée des consommateurs.

Pour comprendre l'impact économique de la réussite ou de l'échec de la Confiance Numérique, nous avons mené une analyse visant à obtenir une vue holistique de l'économie numérique et de ses recettes en Europe, aujourd'hui et plus particulièrement à l'avenir, et à évaluer en chiffres concrets les effets d'une Confiance Numérique solide ou faible. Jusqu'à présent, plusieurs études et comptes-rendus ont montré et estimé l'impact des mesures individuelles dans le domaine de la Confiance Numérique, chacun d'entre eux partant de différentes suppositions et étant valable seulement pour des régions géographiques limitées. Pour notre appréciation, nous avons tiré profit de toutes ces

Illustration 57 : Impact de la Confiance Numérique



Note : PIB Europe 2012 estimé à 12,5–13,5 tn EUR (Europe : UE-27 + Norvège + Suisse
Source : Ovum, analyse Booz & Company

données de départ et bâti un modèle holistique cohérent pour l'ensemble de l'Europe et pour toutes les mesures de la Confiance Numérique.

Cette analyse des risques et bénéfices procure une vue complète indiquant quels piliers de la Confiance Numérique ont le plus grand impact financier. Elle évalue l'impact sur les recettes de l'économie numérique européenne de deux scénarios alternatifs comparés à un cas de base. Concrètement, elle indique en détail à quel degré les pools de revenus de l'économie numérique sont mis en danger par les problèmes de Confiance Numérique, et elle fournit à cette occasion une vue des stimulations financières incitant l'industrie à concentrer son attention sur le développement de solutions favorisant la Confiance Numérique. Comprenant ceci, les gouvernements et les régulateurs peuvent ensuite soutenir les tentatives de l'industrie dans des domaines plus motivés par des intérêts sociétaux que par des intérêts financiers.

L'introduction de services plus interactifs et nécessitant une bande passante plus importante est très sensible à la Confiance Numérique.

La donnée de départ de l'analyse est une grandeur de référence du marché bâtie à partir de statistiques et prévisions multiples provenant aussi bien de conciliations d'experts de Booz & Company et de conclusions tirées d'un programme de plus de 50 entretiens avec des experts de l'industrie que de l'examen en profondeur des meilleures pratiques et des perspectives de l'industrie.

Sur la base d'une revue minutieuse des données acquises, les facteurs clés de l'analyse ont été identifiés et utilisés comme points de départ pour le développement du modèle. Le modèle a été développé selon une approche itérative, en procédant à des analyses de sensibilité pour saisir la variation des facteurs. Le résultat stabilisé du modèle a finalement été récapitulé dans des scénarios cohérents nécessaires pour faire ressortir une vue agrégée des points forts et faibles de la Confiance Numérique.

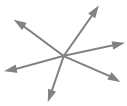
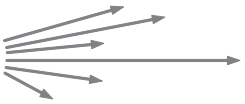
1. RÉSUMÉ FINANCIER : LES RISQUES D'UN RECUL DE LA CONFIANCE NUMÉRIQUE L'EMPORTENT SUR LES BÉNÉFICES POTENTIELS

En point de référence de l'analyse, l'économie numérique européenne[8] est évaluée à un volume de recettes de 436 milliards d'€ pour les quatre catégories majeures de l'accès, du commerce, des contenus et de la publicité pour 2012, avec un taux de croissance composé annuel total de 18 % (2007-2012).

Le scénario le plus pessimiste – l'échec de la Confiance Numérique, défini comme un scénario de « Divergence de l'industrie » – présente un risque

(8) L'Europe est définie dans ce contexte comme l'UE-27 plus la Norvège et la Suisse.

Illustration 58 : Impact de la Confiance Numérique—description du scénario

	Hypothèse basse	Scénario de base	Hypothèse haute
Devise	« Situation de divergence » Différentes mesures ont été prises 	« Business as usual » Mesures plus ou moins synchronisées 	« Une direction » Convergence entre parties prenantes 
Intégrité réseau & QoS	• Utilisation non coordonnée du réseau à l'origine d'une congestion systémique et d'une expérience dégradée des utilisateurs	• Congestion occasionnelle du réseau, en heures de pointe, plus grande attention des ORMS demandée pour une gestion efficace du trafic	• Bande passante beaucoup plus grande avec expérience constamment fiable des utilisateurs
Protection données personnelles	• Consommateurs donnent un nombre plus important de données augmentant les risques de profilage	• Transparence accrue de l'utilisation des données, mais aucune améliortion significative de la menace de phishing/ vol d'identité	• Education, transparence et mécanismes d'opt-in/opt-out pour une plus grande volonté de partage de données (p.ex. publicité innovatrice)
Protection des mineurs	• Efforts pédagogiques parsemés autour des menaces liées à l'Internet pour enfants et parents	• Développer les mesures pédagogiques et de filtrage existantes avec une légère amélioration du processus	• Amélioration et cohérence de l'éducation des parents et mineurs par tous les acteurs • Approche plus disciplinée des mineurs, réseaux sociaux
Prévention piraterie et vol	• Piraterie continuelle et réduction des propositions existantes de contenu légal	• Part significative du partage et du téléchargement illicites de contenus protégés par un droit d'auteur	• Meilleures solutions DRM pour modèles d'affaires traditionnels
Position du régulateur	• Ne donne pas de vision cohérente, cherche à surréguler (ex. exigences de QdS, poursuite de la piraterie)	• Se concentre généralement sur les thèmes les plus graves, notamment les intérêts des différents secteurs (p.ex. sphère privée, protection des mineurs), mais autorise aussi des interventions telles que la « riposte graduée »	• Contribue fortement à l'approche « unidirectionnelle », stimule la gouvernance collaborative conduite par l'industrie

négatif plus grand que le bénéfice obtenu en cas de réussite de la Confiance Numérique – définie comme le scénario « Une direction » : alors que le risque négatif potentiel s'élève à 78 milliards d'€, le bénéfice potentiel est de 46 milliards d'€. L'addition de ces deux chiffres montre un écart de 124 milliards d'€ dans les revenus de l'industrie, ce qui est équivalent à environ 1 % du PIB européen avec des effets correspondants sur les investissements et l'emploi.

Les revenus en danger illustrent la perte potentielle de valeur infligée à tout l'écosystème de l'économie numérique – des consommateurs aux annonceurs, fournisseurs de contenus et opérateurs de réseaux. Dans le cas le plus pessimiste, il y aura moins d'usagers faisant moins et dépensant moins en comparaison par rapport au cas le plus optimiste. Bien que la majorité de ces revenus ne soient pas complètement perdus (parce que seulement déplacés d'Amazon vers les librairies construites en dur), certains modèles économiques et leurs revenus pourraient cependant être complètement perdus (par ex. les enchères en ligne, qui sont plus difficiles à déplacer vers le monde hors ligne).Deux piliers s'appliquant à toutes les catégories de revenus ont l'impact financier le plus grand. Premièrement, la « protection de la vie privée et des données » qui se rapporte aux inquiétudes des consommateurs quant à la sécurité des données numériques. Par exemple, dans le scénario du cas le plus pessimiste, les consommateurs seront moins disposés à partager des informations avec des parties tierces, exerçant ainsi une forte pression sur les modèles de publicité innovants dans lesquels l'industrie du numérique et les vendeurs placent de grandes espérances - en outre, ces modèles de publicité individualisée sont non seulement la base de nombreux modèles économiques B2C, mais ils offrent également des avantages concrets aux consommateurs, par exemple en leur fournissant des informations mieux ciblées facilitant leurs décisions d'achat. De plus, les consommateurs pourraient être moins disposés à utiliser le e-commerce ou à acheter des contenus numériques s'il existe un manque de confiance dans la manière dont sont traitées et gérées leurs données. Deuxièmement, le pilier « intégrité du réseau et qualité du service » a également un impact majeur sur les revenus étant donné qu'il se rapporte à la protection des platesformes technologiques et à la nécessité d'assurer une connectivité Internet optimale permettant la vie numérique. Bien géré, le réseau peut être utilisé pour fournir aux utilisateurs finaux une bande passante élevée à un niveau de qualité qui permet à tous les usagers de profiter de l'entière richesse de la vie numérique – de la téléphonie et la navigation Internet aux services multimédias et à la vidéo à la demande. En tant que tel, le pilier « intégrité du réseau et qualité du service » a un impact direct sur le niveau d'usage et sur le nombre d'usagers et des répercussions dans les catégories majeures de revenus.

Les autres piliers de la Confiance Numérique, bien qu'importants, ont moins d'impacts en termes purement économiques étant donné qu'ils affectent seulement certaines catégories de revenus. La « prévention de la piraterie et du vol » a primairement un impact sur les recettes des propriétaires de contenus. De plus, il existe un risque négatif assez important lié à l'impact négatif sur les transactions de e-commerce chez les personnes substituant les médias traditionnels (par ex. CD et DVD) par l'achat en ligne. La « protection des mineurs » a un effet indirect sur la consommation Internet dans la mesure où les parents contrôlent le niveau quantitatif d'usage de leurs enfants et parce que les enfants eux-mêmes pourraient s'abstenir d'utiliser certaines offres (par ex. les sites de réseaux sociaux) s'ils entendent fréquemment parler d'expériences négatives.

Presque 80 milliards d'€ de recettes du e-commerce sont menacés jusqu'en 2012 en raison de la Confiance Numérique

2. SCÉNARIOS DE LA CONFIANCE NUMÉRIQUE – DE LA DIVERGENCE À LA CONVERGENCE

Les scénarios utilisés pour établir un modèle de l'impact de la Confiance Numérique ont été dérivés de la compréhension générale du sujet par l'industrie, et en particulier des exemples de cas qui illustrent les pratiques liées aux inquiétudes les plus impérieuses. Les trois scénarios varient dans la devise générale et les caractéristiques respectives :

- « Business as usual » (scénario de base) est le point de départ ou la référence de base de l'analyse. Le scénario est caractérisé en ce qu'il suit la trajectoire actuelle, avec seulement des améliorations croissantes dans quelques domaines et des mesures plus ou moins synchronisées entre les parties prenantes. Les activités éducatrices seraient poursuivies à leur niveau actuel ; la transparence dans l'usage des données serait progressivement améliorée, mais il n'y aurait pas d'améliorations significatives par rapport au phishing et aux logiciels malveillants ; en raison d'une mitigation relativement efficace, la qualité du service serait acceptable avec quelques problèmes occasionnels dus à la congestion du réseau ; les défis de maîtrise des contenus protégés par copyright resteraient dans une large mesure en l'état actuel (c.-à-d. le dommage actuel dû à la piraterie fait partie du cas de base).

- « Une direction » est le cas le plus optimiste dans lequel l'industrie adopte une approche harmonisée de la Confiance Numérique, tous les acteurs travaillant de manière cohérente à une vision commune. L'éducation est améliorée de manière significative à tous les niveaux, les parties prenantes joignant fréquemment

leurs efforts dans ce but ; la meilleure compréhension par le consommateur des forces et des faiblesses de la publicité ciblée encourage l'essor de celle-ci ; tirant profit d'une large gamme de mesures acceptées, les opérateurs de réseaux et les fournisseurs de services réussissent à fournir une qualité de service très élevée, avec des vitesses supérieures à celles d'aujourd'hui ; le partage inégal de fichiers décroît étant donné que la prise de conscience du consommateur augmente et que des offres de contenus appropriées émergent, de pair avec de nouveaux modèles économiques intelligents.

Le e-commerce, les contenus et la publicité sont les domaines les plus exposés aux risques liés au recul de la Confiance Numérique.

- « Divergence de l'industrie » est le cas le plus pessimiste pour l'économie numérique étant donné qu'il inhibe la continuité de croissance de l'économie numérique. Dans un tel scénario, les acteurs agissent de manière indépendante, l'absence d'une vision commune a pour résultat un grand nombre de mesures diverses appliquées de manière incohérente. Les mesures de protection des mineurs dans les environnements numériques sont limitées et souvent contradictoires ; étant donné que les consommateurs sont confrontés à des problèmes de non-respect de la vie privée, leur scepticisme augmente face à l'industrie du numérique en général ; la gestion incontrôlée du trafic entraîne de fréquents problèmes de qualité du service et des plaintes relatives à l'absence de neutralité du net ; les problèmes autour des contenus sous copyright grandissent considérablement, et la « dépression » générale de l'industrie des contenus entraîne une réduction des offres de contenus légaux dans le monde numérique.

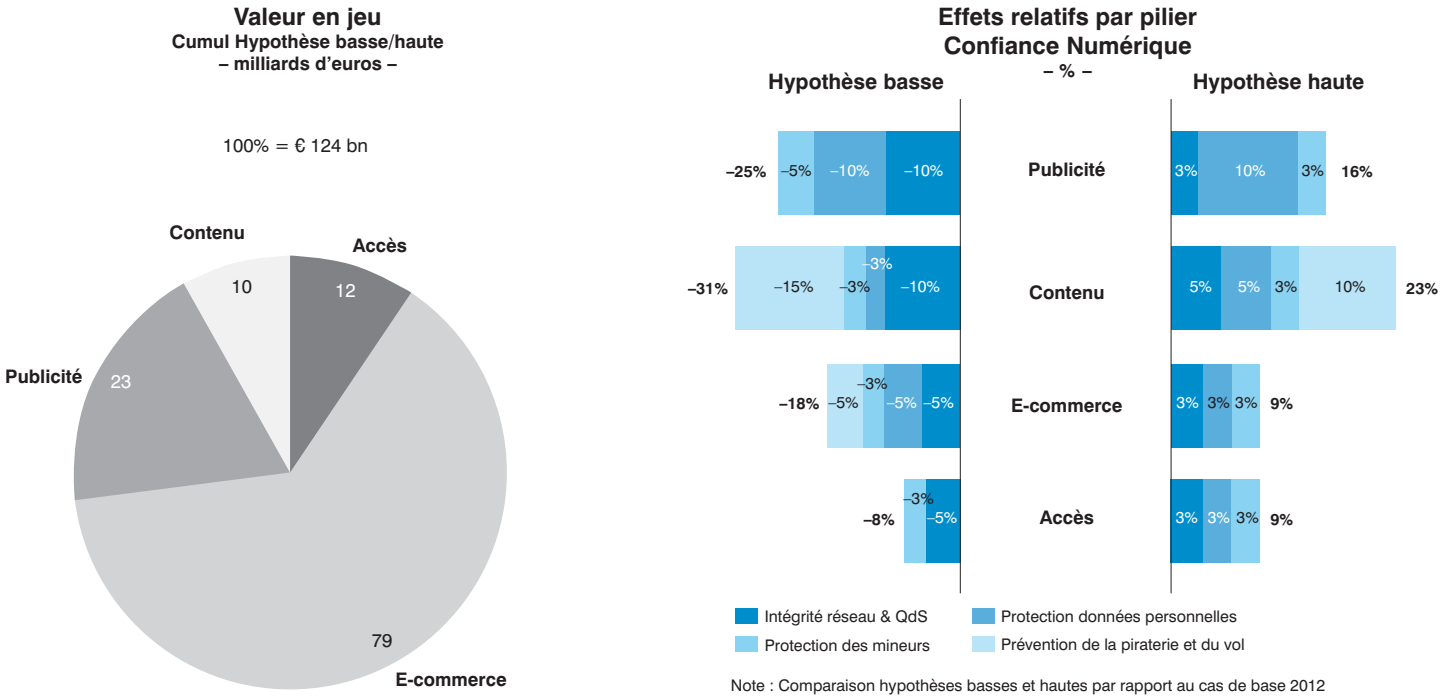
La distinction essentielle entre les scénarios est le degré d'alignement entre les acteurs de l'industrie dans leur approche de la Confiance Numérique. L'alignement ne signifie pas nécessairement que les acteurs doivent agir en tout point de manière identique ; il s'agit plutôt du degré d'accord au sein de l'industrie en vue de prendre la même direction. Cela se rapporte à la mesure dans laquelle il existe une entente commune concernant une telle direction à prendre et aux priorités globales aussi bien qu'aux responsabilités en résultant pour chaque partie prenante.

Les degrés plus élevés de jonction des responsabilités –par exemple dans le cas le plus optimiste – entraînent une amélioration dans l'application de la Confiance Numérique au sein de chacun des piliers, donc un soutien de l'usage et, de manière subséquente, la croissance des revenus.

3. FACTEURS CLÉS FINANCIERS : LA PUBLICITÉ ET LES CONTENUS SONT LES PLUS SOUMIS À LA CONFIANCE NUMÉRIQUE

Les catégories de revenus les plus fortement menacées par rapport à la Confiance Numérique sont les contenus et la publicité.

Illustration 59 : Impact de la Confiance Numérique—zones de croissance et piliers



Note : Comparaison hypothèses basses et hautes par rapport au cas de base 2012

Les contenus sont hautement sensibles aux niveaux de Confiance Numérique. Ceci peut déjà être constaté par exemple au niveau de l'impact financier de la piraterie vidéo aujourd'hui – hors ligne et en ligne. Pour 2007, la MPAA (Motion Picture Association of America) évalue une perte de plus de 18 milliards de $ dans le monde en raison de la piraterie, cette somme représentant seulement le dommage direct sans considérer les impacts économiques indirects potentiellement plus grands. Avec 31 % de revenus en danger dans le cas le plus pessimiste de Confiance Numérique, il est nécessaire que les entreprises et les consommateurs aient confiance et espèrent que les plates-formes de contenus en ligne pourvoient les propriétaires de contenus tout en procurant un environnement sécurisé pour ce qui est des données personnelles des usagers (par ex. historique de l'usage, enregistrement des données de cartes de crédit, etc.). Par ailleurs, étant donné que les contenus, dans de nombreux cas, nécessitent une livraison en temps réel (par exemple le iPlayer de la BBC et d'autres solutions de streaming de vidéos à la demande), ils sont hautement dépendants de la qualité de l'infrastructure sous-jacente du réseau. La faculté de dériver des profits et de faire croître les revenus liés aux contenus sera dépendante de la qualité du réseau fourni par les opérateurs de réseaux. En tant que tels, les fournisseurs de réseaux et de contenus devront trouver un modèle permettant de répartir les coûts et les revenus de manière équitable, et fournir ainsi les stimulations appropriées pour les investissements d'infrastructure nécessaires en vue de faire de l'Internet un média de distribution grand public des contenus. Dans le cas le plus optimiste, 4 milliards d'€ de revenus supplémentaires peuvent être atteints, comparés à un risque négatif de 6 milliards d'€.

La publicité est également hautement dépendante de la confiance des consommateurs, étant donné que les annonceurs continueront seulement à déplacer leurs investissements des environnements traditionnels vers les environnements numériques si l'usage et le temps passé en ligne continuent de croître. Pour la publicité, le potentiel positif est de 9 milliards d'€, le risque négatif de 14 milliards d'€. Cela signifie que presque 25 % des recettes publicitaires sont menacées dans le scénario le plus pessimiste.

En termes absolus, c'est le e-commerce qui est le plus menacé dans le contexte de la Confiance Numérique étant donné qu'il est de loin la catégorie de revenus la plus grande. Le risque négatif est de 52 milliards d'€, tandis que le potentiel positif s'élève à la moitié. En termes relatifs cependant, le e-commerce est moins touché, étant donné que la confiance placée dans les acteurs bien établis (par ex. Amazon) est déjà raisonnablement élevée et que les biens font l'objet d'une livraison physique, n'étant ainsi pas dépendants de l'Internet dans l'exécution réelle de la prestation.

En tant que catégorie de revenus sous-jacents, l'accès est le moins influencé par la Confiance Numérique. Les prévisions de croissance sont plus faibles pour l'accès, qui sont de plus en plus standardisés. Le succès ou l'échec de la Confiance Numérique n'influencera probablement pas significativement le nombre des usagers. Le risque négatif et le potentiel positif ont la même valeur évaluée à 6 milliards d'€. L'Illustration 58 résume les risques négatifs et les potentiels positifs pour le cas le plus pessimiste et le cas le plus optimiste.

4. CONCLUSION

Pour parler en termes purement économiques en laissant de côté pour le moment les aspects sociétaux plus larges, l'analyse des risques et des bénéfices montre que l'industrie numérique a une motivation économique considérable devant l'inciter à aborder de manière cohérente certains domaines de la Confiance Numérique, au moins pour éviter le scénario le plus pessimiste en termes de revenus et, dans l'idéal, pour atteindre le potentiel de recettes du cas le plus optimiste. Premièrement, la « protection de la vie privée et des données » est financièrement importante, spécialement mais non exclusivement en raison de ses implications dans des modèles économiques de publicité innovante (ciblée). Deuxièmement, l' « Intégrité du réseau et la qualité du service » seront nécessaires pour soutenir la continuité de la croissance des services de contenus et de vidéos. Troisièmement, le domaine de la « Prévention de la piraterie et du vol » est pertinent aussi bien pour les propriétaires de contenus que pour le e-commerce. Mis à part les implications évidentes en termes de recettes pour l'industrie des contenus pour ce qui est de protéger la valeur existante de leurs portefeuilles de droits et d'introduire des modèles économiques innovants de contenus numériques et en ligne, il existe un risque négatif supplémentaire non négligeable lié à l'impact négatif sur les transactions de e commerce en raison des personnes déplaçant leur consommation vers des chaînes et sites hors ligne, ce qui n'est pas possible pour un grand nombre de modèles économiques nouveaux (par ex. enchères en ligne).

En résumé, les fournisseurs de réseaux doivent continuer à jouer un rôle important étant donné que leur cœur d'activité est un élément clé pour les facteurs de croissance économique identifiés. Le degré d'intégrité des réseaux a un impact économique majeur même si leur propre noyau, l'accès, semble moins exposé aux bénéfices et aux risques liés à la réussite ou à l'échec de la Confiance Numérique.

VI. CADRE D'ACTION

1. L'INDUSTRIE DOIT PARVENIR À UNE POSITION DE LEADER DANS LA CONFIANCE NUMÉRIQUE

L'économie numérique européenne a une perspective réaliste de croissance aiguillonnée par les services de type Web 2.0 qui sont devenus la tendance dominante en utilisant la fonctionnalité, l'omniprésence et la capacité augmentée des réseaux haut débit. La transition vers des réseaux d'accès nouvelle génération, la prolifération de technologies basées sur le réseau et hautement sophistiquées et la nouvelle génération de consommateurs « nés à l'ère du numérique » et dotés d'une très grande assurance constituent des forces potentiellement perturbatrices pour l'écosystème de l'économie numérique. Ce nouveau paradigme est un défi considérable aussi bien pour l'industrie au sens large que pour les responsables des politiques appliquées et les régulateurs. Le degré de confiance accordé par les consommateurs aux fournisseurs de services et de plates-formes en termes de maintien du service et de fourniture d'environnements de réseaux et de services sécurisés, aussi bien que celui accordé au gouvernement et aux autorités de régulation quant à l'aptitude à faire respecter les standards de protection des consommateurs, est en train de devenir rapidement un paramètre majeur pour l'aptitude à réaliser effectivement le potentiel de croissance de l'économie numérique.

L'industrie se trouve à un tournant dans le développement de l'économie numérique. L'analyse des risques et bénéfices montre à quel point l'industrie est touchée par l'impact financier de la Confiance Numérique. Il existe un impératif financier clair devant inciter à l'action, avec 124 milliards d'Euros menacés à l'échelle de toute l'industrie. Toutefois, outre les motivations financières, l'extension des références de la Confiance Numérique est également une responsabilité sociale étant donné qu'il s'agit là d'une sphère globale d'inquiétudes pour les consommateurs, les régulateurs et la société.

Les études de cas du présent rapport confirment que ces inquiétudes sont aujourd'hui abordées par les diverses parties prenantes de l'industrie. Cependant, ces actions sont extrêmement sensibles et dictées par la nécessité de réagir aux protestations du public et à la pression des médias et des organes de régulation résultant des incidents sévères au niveau de la sécurité des données, du respect de la vie privée ou d'autres types de violation de la confiance. Les violations de la confiance ont été jusqu'ici provoquées, entre autres, par :

- Des attentes non gérées relatives au niveau de service, par ex. lors de promesses surfaites concernant les prestations – bien que la réalisation de telles promesses ne soit pas entièrement sous le contrôle de l'opérateur de réseaux – comme dans le cas des FAI américains qui avaient communiqué qu'aucun contenu de pornographie enfantine ne serait accessible sur leur réseau. Comme autres exemples, on peut citer les cas où des usagers ont connu une dégradation de services très appréciés nécessitant une bande passante importante (tels que les sites P2P de partage de fichiers) par le déploiement de technologies de gestion des réseaux.

- Des attentes non gérées concernant l'efficacité du filtrage dans le cas des contenus de pornographie enfantine.

- L'usage de technologies intrusives pour une surveillance de l'Internet à des fins commerciales.

Malgré la complexité et la diversité des méthodes actuelles, plusieurs grandes lignes prennent forme concernant les meilleures pratiques, du point de vue de l'acceptation par le consommateur :

- Les consommateurs acceptent les pratiques qui sont transparentes et qui s'avèrent discrètes : les opérateurs de réseaux et les fournisseurs de contenus et de plates-formes, conjointement avec les organes de régulation, se doivent de faire avancer une telle communication.

- Les consommateurs sont préoccupés par la question de savoir comment les opérateurs de réseaux gèrent et protègent les données numériques des consommateurs : des déclarations claires et une structure de régulation consistante et fiable semblent être ici une priorité absolue.

- Les consommateurs exigent un contrôle des risques auxquels ils sont exposés : ceci rend nécessaire un accès aux outils adéquats, des mécanismes opt-in/opt-out et une certaine éducation du consommateur.

• Les consommateurs acceptent les mesures qui garantissent un service de qualité : si ceci requiert une gestion active des opérations, ils sont alors ouverts à une telle démarche, à condition que les conditions du service soient communiquées ouvertement, que les prix soient équitables et transparents et qu'il n'y ait aucune discrimination dans l'accès.

Les analyses de cas montrent également le degré de complexité impliqué si l'on veut que la Confiance Numérique fonctionne. Même des solutions bâties sur les meilleures intentions, visant la prévention de certains comportements par le blocage ou le filtrage de contenus, peuvent être jugées en conflit avec les libertés civiles et les exigences de neutralité de l'Internet. Les solutions qui se concentrent sur l'éducation et la responsabilisation du consommateur – pour que celui-ci comprenne les risques et prenne la responsabilité d'agir pour gérer ces risques – exigent un degré élevé d'implication de la part de l'industrie afin d'encourager la prise de conscience. Les outils logiciels sont disponibles et aptes à soutenir les deux méthodes, mais une définition commune des standards et des politiques vis-à-vis des contenus inadéquats est cependant nécessaire.

Les quatre piliers de la Confiance Numérique doivent être abordés pour maintenir la croissance de l'économie numérique.

Pour éviter les réponses géographiquement dispersées et fragmentées aux problèmes de confiance numérique qui deviennent de plus en plus globaux et vastes, nous en appelons à une approche holistique et à un large alignement de l'industrie. Ceci mènera finalement à une plus grande transparence et à une plus grande assistance du consommateur au sujet des risques et des bénéfices de l'économie numérique.

Chacun des piliers de la Confiance Numérique est complexe, au niveau des menaces et des solutions comme au niveau des positions et intérêts des diverses parties prenantes.

Le sujet est essentiellement exploré du point de vue de l'opérateur de réseau. Son positionnement souhaité par rapport à la Confiance Numérique est défini, et les mesures appropriées sont détaillées en conséquence. La discussion est ensuite ramenée au niveau de l'industrie par l'identification des implications pour les parties prenantes, et en particulier pour les organes de régulation.

2. LES OPÉRATEURS DE RÉSEAUX ET LES FAI DOIVENT ADOPTER UNE POSITION CLAIRE VIS-À-VIS DE LA CONFIANCE NUMÉRIQUE

L'idée globale que se fait un fournisseur de réseau ou un FAI de lui-même joue un rôle important dans la définition du degré d'engagement à établir des politiques proactives visant la Confiance Numérique : sommes-nous seulement un « simple tuyau », nous contentons-nous d'ouvrir la voie et d'exploiter les autoroutes ? Ou bien souhaitons nous nous engager réellement dans l'établissement de règles de transit sur ces autoroutes et maintenir l'ordre dans ces règles ?

Il n'existe cependant aucune réponse unique – la position adoptée par un opérateur de réseau ou par un FAI est fréquemment différente selon les piliers de la Confiance Numérique.
Le cadre de positionnement de la Confiance Numérique est une structure permettant de déterminer les positions des piliers de la Confiance Numérique aussi bien individuellement que globalement. L'axe vertical différencie les principes sous-jacents, « volontaire » et « obligatoire » en sont les deux pôles. L'axe horizontal différencie la manière dont sont prises les mesures, passivement selon le principe de la « non-intervention » ou activement selon une méthode de « plein contrôle ». Les quatre cadrans qui en résultent peuvent être symboliquement reliés à des archétypes de rôles sociétaux. L'Enseignant éduque autant que possible les utilisateurs au sujet des opportunités et des menaces, mais ne prendra normalement aucune mesure corrective active. Le Parent éduque les utilisateurs au sujet des menaces et des mesures de manière similaire à l'Enseignant, mais prendra des mesures de manière proactive si cela est jugé nécessaire. Le Juge se base sur une mise en application auto-imposée de règles au cas par cas et sur des directives plutôt que sur l'éducation seule, mais les règles sont basées sur des accords mutuels. Le Policier est naturellement enclin à une mise en application forte, il prend toutes les mesures nécessaires et agit en se basant sur des règles strictes, par ex. en bloquant toutes les activités illégales.

Sur la base de notre recherche et de notre compréhension de l'industrie confirmées par notre programme d'entretiens, il apparaît clairement que l'environnement habituel et naturel des FAI, leur « terrain connu », a été jusqu'ici le cadran supérieur gauche : le rôle de l'Enseignant. Les caractéristiques associées à ce cadran sont en concordance avec l'idée primaire que se fait un opérateur de réseau de lui-même : le cœur de son activité a toujours été et est encore de fournir un réseau sûr, fiable et puissant pour le trafic Internet, sans s'impliquer dans ce qui se déroule sur son réseau. De ceci peut être dérivé un rôle d'éducateur sensibilisant les consommateurs quant aux problèmes de confiance numérique tout en leur fournissant les outils pour gérer ces problèmes sur la base d'une approche non interventionniste. Un tel positionnement limite les risques

et les responsabilités juridiques par rapport à des problèmes dont le FAI n'est pas primairement responsable. En général, le FAI ne prendrait pas en charge de lui-même la définition ou l'application de standards de la Confiance Numérique, par exemple par l'engagement de poursuites contre les violations de copyright. Cependant, notre analyse montre également que ceci n'est pas suffisant. Étant donné qu'une part significative de la croissance future est liée à un plus fort usage de services numériques et en ligne déjà existants ou nouveaux à valeur ajoutée, le degré de confiance accordé par les consommateurs à leur fournisseur d'accès devient un préalable majeur de la croissance et du succès sur le marché numérique. En tant que FAI, il n'est pas suffisant de s'en remettre uniquement à l'éducation, aux programmes de responsabilités d'entreprise et à l'observation des lois pour obtenir l'acceptation des usagers et construire la confiance. Fréquemment, la législation ne peut pas faire face à elle seule à la rapidité et à l'envergure des changements, par ex. au sein des nouvelles technologies de surveillance du trafic ou des risques accrus de sécurité liée à la sophistication de la cybercriminalité qui a un impact sur la Confiance Numérique. De ce fait, les entreprises qui réussissent ne se contentent pas de se conformer à la législation, elles essaient en outre d'avoir une longueur d'avance en adoptant des politiques et des pratiques proactives pour gérer la Confiance Numérique.

- Elles intériorisent la confiance en établissant des procédures et des protocoles.

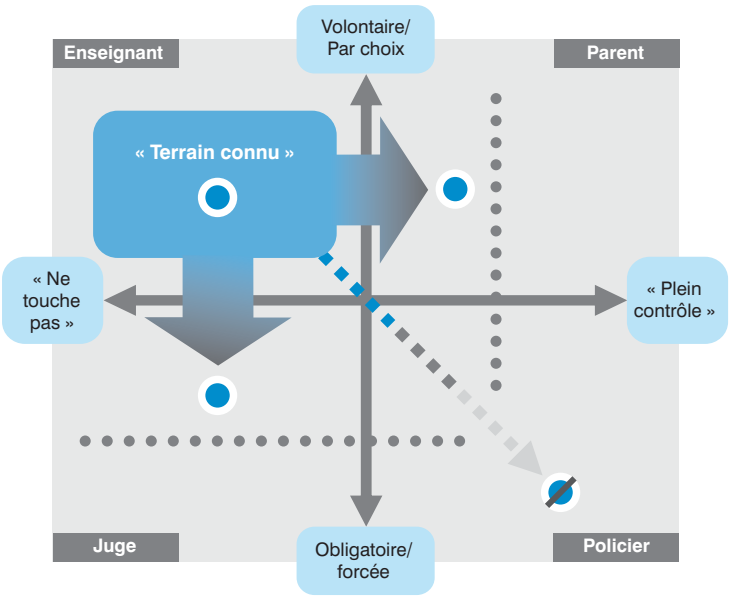
- Elles sont aussi ouvertes et transparentes que possible dans leur communication avec les consommateurs.

- Elles accomplissent un effort supplémentaire pour éduquer les consommateurs et leur permettre de protéger leurs intérêts au sein de l'univers numérique.

- Elles utilisent une approche progressive et proactive en appliquant le paradigme « ERI » suivant : éduquer d'abord, responsabiliser ensuite, puis imposer uniquement si cela est faisable.

En tant que tels, les MNO doivent déterminer de manière proactive les ordres du jour de l'industrie, en cherchant à développer des solutions et des approches qui les amèneront inévitablement à de nouvelles positions : celles des rôles du Parent et du Juge. Il existe un certain nombre de motivations pour les opérateurs de réseaux et les FAI les incitant à sortir de leur environnement habituel.

Illustration 60 : Positions des opérateurs de réseaux



Premièrement, des raisons fortement stratégiques ou d'affaires pourraient amener l'opérateur de réseau ou le FAI à quitter son environnement habituel, par ex. pour s'assurer la bienveillance des consommateurs. Par exemple, si les parents sont satisfaits du niveau de protection de leurs enfants, ils les autoriseront à utiliser l'Internet plus souvent. La gestion de trafic est également un élément de valeur stratégique étant donné qu'elle garantit que tous les consommateurs profitent des investissements dans les réseaux d'accès de nouvelle génération et leur bande passante accrue, et non pas seulement les utilisateurs lourds. La mesure dans laquelle un opérateur de réseau est apte à garantir la qualité du service et une bande passante optimale à tous les usagers est un outil concurrentiel essentiel au sein de la concurrence des infrastructures.

Deuxièmement, pour anticiper l'intervention régulatrice potentiellement disproportionnée par l'encouragement d'une meilleure autorégulation et coopération de l'industrie. Par exemple, comme ceci fut annoncé au Royaume-Uni où les FAI leaders coopèrent avec la British Phonographic Industry pour aborder activement les consommateurs et les mettre en garde contre la piraterie. Aux États-Unis, Comcast est parvenu à un accord constructif avec BitTorrent sur une politique de gestion du trafic mutuellement acceptable.

Les FAI doivent cependant être très prudents dans de tels mouvements, dès qu'il s'agit pour eux d'assumer des rôles en dehors de leur sphère primaire de responsabilités. Tout mouvement susceptible d'ébranler leur havre sûr de « simple tuyau » et de les exposer à des responsabilités

incontrôlables annihilera, en fin de compte, leur contribution à l'amélioration de la confiance numérique – bien que les attentes au sein du public eussent été augmentées. Sans mentionner les signaux négatifs que ceci enverrait à leurs investisseurs et à leurs actionnaires.

Les FAI devraient dans tous les cas éviter de se déplacer vers le rôle de Policier à moins d'y être obligés par la loi. Le rôle du Policier est une approche hautement oppressante qui aurait un impact négatif sur l'acceptation par les consommateurs. Si une obligation légale est imposée, les opérateurs de réseaux et les FAI sont toutefois d'une part contraints d'assumer un tel rôle, mais d'autre part également protégés contre les responsabilités légales s'ils agissent ainsi. Par exemple, s'ils sont contraints par la loi de bloquer certains sites Internet (en raison de problèmes de contenu), ils ont alors moins menacés d'accusations de violation de copyright, de non-respect des libertés civiles, de la liberté d'expression ou de la neutralité du net.

L'industrie devrait appliquer le paradigme ERI : Éduquer, Responsabiliser, Imposer.

Pour résumer, ce positionnement est traduit par un paradigme clair : ERI – Éduquer, Responsabiliser, Imposer. Le positionnement sur la matrice détermine le niveau auquel ces rôles sont appliqués dans le cas de l'opérateur de réseau.

3. LES OPÉRATEURS DE RÉSEAUX RÉCLAMENT L'ACTION : LES CINQ INITIATIVES CLÉS EN VUE DE LA CONFIANCE NUMÉRIQUE

Le paradigme ERI définit de manière résumée ce qu'un opérateur de réseau ou un FAI doit faire, mais il est tout aussi applicable aux autres parties prenantes de l'industrie du numérique.

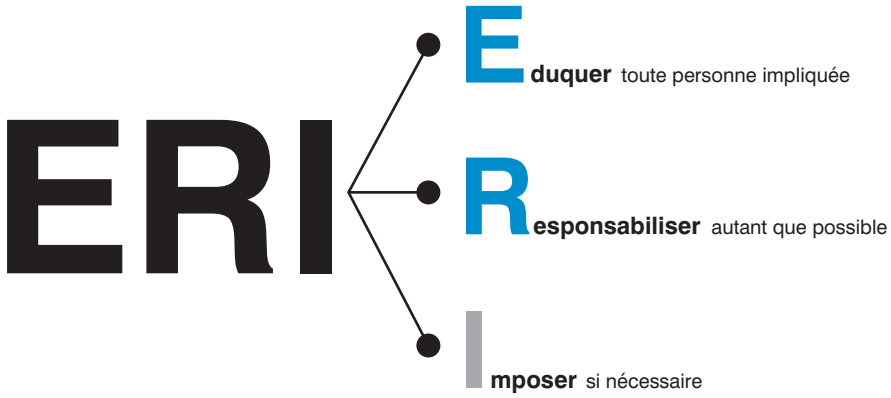
Éduquer : les opérateurs de réseaux et les FAI doivent s'assurer que leurs clients comprennent les menaces qui entourent l'industrie du numérique et doivent leur fournir les connaissances permettant de gérer ces menaces et donc d'agir en toute sécurité au sein de cet univers. Les politiques doivent être claires et transparentes pour les utilisateurs finaux. Ceux-ci englobent la transparence au sujet des politiques d'entreprise dans le domaine de la Confiance Numérique.

Responsabiliser : les opérateurs de réseaux et les FAI doivent permettre autant que possible à leurs clients de contrôler par eux-mêmes les menaces numériques et les problèmes, par ex. grâce à une méthode opt-in ou opt-out pour bloquer les contenus indésirables. En particulier, les opérateurs de réseaux et les FAI doivent fournir aux clients de tels processus et outils et soutenir les parties tierces dans le développement et l'exploitation de ces outils et services.

Imposer : les opérateurs de réseaux et les FAI doivent intervenir et diriger de manière proactive le comportement des utilisateurs dans les domaines spécifiques d'intérêts publics vitaux pour préserver la confiance numérique. Les FAI doivent, dans ces domaines, chercher à atteindre un alignement à l'échelle du secteur et partager les meilleures pratiques.

Le fait de mettre un accent fort sur l'éducation et la responsabilisation permet de favoriser efficacement les changements dans l'idée que les consommateurs se font d'eux-mêmes et dans la manière dont ils s'informent et dont ils abordent les problèmes. Une enquête récente (Baromètre de Confiance Edelman 2008) analysant les « jeunes décideurs » européens, les jeunes leaders d'opinion âgés de 25 à 34 ans, conclut que ces jeunes décideurs se procurent leurs informations d'une manière profondément différente de leurs aînés, en se fiant à de multiples sources d'information et en modelant leurs points de vue par une participation, une réflexion et un partage constants. En tant que tels, les jeunes

Illustration 61 : *Le paradigme ERI*



décideurs sont ouverts et même exigent d'être correctement éduqués et responsabilisés afin de pourvoir à eux-mêmes. L'enquête constate qu'ils ont aujourd'hui tendance – malgré le fait qu'ils soient « historiquement cyniques vis-à-vis des entreprises » – à témoigner un degré comparativement élevé de confiance envers les entreprises. Mais les sources d'informations les plus dignes de confiance pour les jeunes décideurs dans la majorité des pays de l'UE sont les « personnes comme vous et moi » et les ONG. Les opérateurs de réseaux et les FAI peuvent bâtir là-dessus non seulement pour aborder les problématiques de la Confiance Numérique, mais également pour en tirer profit comme contribution dans le but de retenir la clientèle classique.

Bâtissant sur cette grande ligne générale, une vision orientée sur l'entreprise est mise en place pour dériver et spécifier des mesures concrètes. Les mesures ont été définies dans cinq domaines d'initiative :

1. POLITIQUES ET PROCÉDURES

Les opérateurs de réseaux et les FAI doivent affirmer leur positionnement vis-à-vis de la Confiance Numérique en définissant leur stratégie et leur position pour chaque pilier de la confiance. Ceci doit être le fondement de toutes les politiques liées à la Confiance Numérique dans quatre domaines : la protection des mineurs, la protection des données et de la vie privée, la gestion des trafics et la piraterie. Cette affirmation de positionnement doit être suffisamment précise pour fournir une direction tangible sur les questions sous-jacentes liées à ces problématiques – par ex. définir comment une entreprise parvient à un équilibre dans le compromis entre les contenus inappropriés et la liberté d'expression.

Dans une démarche suivante, ces politiques doivent être intégrées aux processus centraux de l'entreprise. Dans la majorité des cas, ceci aura un impact direct sur la manière dont les opérateurs de réseaux appréhendent le développement des produits, par ex. en s'assurant que tous les produits et services lancés répondent aux propres standards de l'entreprise.

De plus, les opérateurs de réseaux doivent maintenir à jour les politiques et procédures de la Confiance Numérique, en effectuant des remaniements réguliers des procédures et politiques légales, publiques et techniques existantes.

Enfin, dernier point mais non le moindre, les cas analysés dans ce rapport apportent un enseignement particulièrement important : la confiance est synonyme de foi, et la meilleure base pour cette foi est une communication ouverte ; la transparence est vraiment payante. En conséquence, les entreprises devraient se montrer ouvertes au sujet des politiques qu'elles appliquent et des logiques sur lesquelles elles se fondent – y compris les logiques économiques. L'expérience montre que l'acceptation par le consommateur est généralement élevée lorsque les règles et les logiques sous-jacentes sont ouvertement communiquées – comme dans l'exemple du Gmail de Google qui affiche des publicités ciblées. Ceci permet en outre d'engager avec le consommateur un dialogue qui peut être très utile pour améliorer les solutions.

2. GOUVERNANCE

Les questions de Confiance Numérique sont complexes, très sensibles et interfonctionnelles par nature. Très fréquemment, il est nécessaire de définir exhaustivement les positions fondamentales de l'entreprise – par ex. comment traitons-nous les contenus de pornographie enfantine ? Négliger ceci implique des risques élevés au niveau financier comme au niveau de la réputation. De ce fait, il est extrêmement important de consacrer au sujet l'attention requise et une gestion de pointe. La Confiance Numérique doit être clairement intégrée à la structure organisationnelle, par exemple par le biais d'un Conseil de la Confiance Numérique doté d'une surveillance senior incluant une autorité de supervision et d'implémentation de toutes les activités en rapport.

3. TECHNOLOGIE

Les technologies permettant la Confiance Numérique sont largement mises en place, et l'attention principale doit être accordée aux décisions de positionnement individuel, de définition de politiques appropriées et d'établissement des structures de gouvernance encadrant le tout. Toutefois, la majorité des opérateurs de réseaux auront besoin de faire certains investissements sur le plan technologique afin de préparer le futur. Ceux-ci visent à assurer le maintien de la qualité du service malgré une augmentation du trafic multimédia. Les opérateurs de réseaux devront prendre des décisions d'investissement en gérant le compromis nécessaire entre un élargissement des capacités de transport et la gestion active du trafic, notamment par le biais de prix échelonnés ou de mesures techniques. Les opérateurs de réseaux et les FAI doivent coopérer avec les fournisseurs de contenus afin d'optimiser leurs réseaux pour la fourniture de contenus multimédias grâce à des technologies telles que les caches pair-à-pair (par ex. l'initiative P4P) ou des réseaux de fourniture de contenus.

Ils doivent s'assurer que les régulateurs comprennent bien qu'ils abordent la question de manière appropriée.

Un autre domaine de risque majeur sur le plan technologique s'avère être actuellement la question de l'équipement des utilisateurs finaux. Généralement, cet équipement n'est pas suffisamment protégé contre les menaces telles que les virus, les botnets et autres formes de logiciels malveillants. Il existe déjà des logiciels apportant une solution ; cependant, les fournisseurs de réseaux devraient encourager plus activement les clients à utiliser ceux-ci. Les opérateurs de réseaux et les FAI doivent par ailleurs déployer des outils et des solutions permettant aux consommateurs de contrôler et de gérer leur propre degré d'exposition, par ex. par le biais de fonctions opt-in/opt-out. Ceci rendra nécessaire un changement au niveau des activités : il n'est pas suffisant d'offrir des solutions pour le téléchargement sur le site Web ; les FAI devraient en outre lancer des programmes permettant de gérer et de suivre le nombre de solutions installées (en particulier par l'élargissement de leur rôle d'Enseignant en allant plus vers une position de « Parent »).

4. ÉDUCATION DU CONSOMMATEUR

Les opérateurs de réseaux câble et télécoms et les FAI devraient s'engager dans des programmes d'industrie conjointement avec les ONG et prendre leurs propres initiatives pour une éducation appropriée (par ex. campagnes d'information sur leur propre site Web).
Ces programmes doivent informer exhaustivement des menaces en relation avec la publication de données, la publicité ciblée, la piraterie et le comportement en ligne d'une manière générale (y compris ce que sont le harcèlement, la sollicitation ou les contenus inacceptables). L'éducation doit être faite de manière ciblée avec des messages spécifiquement adaptés aux groupes d'utilisateurs respectifs, y compris aux parents et enfants. Le programme pour parents devrait se concentrer sur la question de savoir comment surveiller les activités des enfants et favoriser la prise de conscience des menaces provenant de l'environnement – de même qu'il devrait montrer aux parents les outils dont ceux-ci disposent pour gérer l'environnement en ligne de leurs enfants. L'éducation des enfants devrait se concentrer sur la reconnaissance et la gestion des menaces.

5. RÉGULATION

Les opérateurs de réseaux doivent encourager les instances de régulation à mettre l'accent sur des domaines spécifiques d'action afin de soutenir les efforts de l'industrie visant à établir la confiance de manière proactive dans des domaines clairement situés hors des attributions et activités des opérateurs de réseaux ou des FAI (comme l'établissement de listes noires des contenus illégaux ou la mise en application de lois). Les régulateurs devraient prendre soin de ne pas instaurer des réglementations obligatoires de manière proactive dans ces domaines à moins que l'adéquation de telles mesures soit assurée. Les régulateurs devraient seulement être directement impliqués lorsque les intérêts des consommateurs sont réellement compromis.

En réponse, l'industrie doit démontrer qu'elle prend la Confiance Numérique au sérieux en prenant l'initiative de développer des solutions cohérentes. Ces solutions doivent obtenir le soutien de tous les acteurs et doivent répartir de manière proportionnée les coûts d'implémentation et les retombées financières positives qui en résultent. Les régulateurs doivent autoriser l'industrie à développer de telles solutions, promouvoir la coopération des parties prenantes et les programmes de soutien financier, en autorisant la pression concurrentielle afin de favoriser le respect des intérêts des consommateurs plutôt qu'en appliquant une régulation qui, malgré ses bonnes intentions, pourrait s'avérer en réalité contre-productive du point de vue du consommateur et entraîner un dommage économique.

Pour l'exécution des mesures correspondant à ces cinq domaines d'initiative, les opérateurs de réseaux et les FAI ont généralement tout intérêt à coopérer le plus possible avec les ONG. De nombreux aspects peuvent être abordés de manière nettement plus efficace lorsqu'un opérateur prend l'initiative conjointement avec une ONG, étant donné que cette dernière peut assurer la neutralité et l'applicabilité à l'échelle de l'industrie en mettant à profit la bonne réputation générale des ONG. Des enquêtes récentes ont montré que les ONG bénéficient d'un degré élevé de confiance de la part des consommateurs.

4. IMPLICATIONS POUR LES AUTRES PARTIES PRENANTES

Cette position de l'opérateur de réseau établit également des attentes claires envers les autres parties prenantes au sein de l'écosystème de l'économie numérique. Les deux groupes les plus importants sont :

- Les consommateurs.

- Les autres fournisseurs sur toute la chaîne de valeur numérique (comprenant les fournisseurs de

contenus, les développeurs et les distributeurs de logiciels et d'applications, par ex. magasins en ligne).

CONSOMMATEURS

Les consommateurs doivent comprendre la nécessité d'utiliser leur bon sens dans l'univers numérique tel qu'ils le font naturellement dans le monde hors ligne. De plus, ils doivent apprendre comment exploiter les solutions orientées vers le consommateur qui sont développées par les opérateurs de réseaux, les FAI et autres pour leur permettre de gérer et de contrôler eux-mêmes les menaces de l'univers numérique. Comme soutien dans ces nécessités, ils devraient accepter et utiliser les offres d'éducation des institutions publiques (par ex. écoles, universités, organismes gouvernementaux).

Les consommateurs doivent apprendre à utiliser les ressources fournies par l'industrie.

LES FOURNISSEURS DE CONTENUS SOUS COPYRIGHT DEVRAIENT PRENDRE DEUX VOIES PRINCIPALES POUR MENER À DESTINATION LEURS ORDRES DU JOUR

Les propriétaires de contenus devraient prendre eux-mêmes la responsabilité de garantir que leurs contenus sous copyright sont adéquatement protégés. L'industrie de la musique a lutté pendant un certain temps pour développer des modèles économiques incorporant les contrôles nécessaires à la prévention de la piraterie. Aujourd'hui, cette problématique touche également les industries du film et de la télévision du fait de la disponibilité de largeurs de bande accrues et de technologies de compression. Les propriétaires de contenus doivent développer conjointement des solutions pour réaliser des valeurs équitables avec les contenus qu'ils possèdent. Pour parvenir à ceci, il leur est nécessaire de développer des solutions de protection des copyrights à un niveau industriel. L'industrie des contenus ne peut pas compter uniquement sur les acteurs des réseaux pour protéger les contenus à leur place. En outre, les consommateurs sont moins disposés à accepter des solutions mises en place par les acteurs de l'Internet (par ex. le filtrage ou le blocage de contenus) lorsque celles-ci ont des motivations purement commerciales comme ce serait le cas pour la protection contre la piraterie, en comparaison avec les solutions ayant également un aspect moral ou social (par ex. le blocage de contenus de pornographie enfantine). Les solutions contre la piraterie doivent englober des modèles économiques innovants aussi bien que des techniques numériques de gestion des droits.

LES AUTRES ACTEURS TIERS DOIVENT COOPÉRER AVEC L'INDUSTRIE INTERNET

Les sociétés du e-commerce devraient travailler en coopération avec les opérateurs et les FAI à des programmes d'éducation communs autour de thèmes présentant un intérêt mutuel (par ex. le phishing). L'intention de tels programmes doit être d'augmenter la confiance des consommateurs par une connaissance améliorée des menaces et des problématiques. Il est également nécessaire de fournir aux consommateurs les outils à même de gérer ces risques. Par conséquent, les opérateurs de réseaux et les FAI ont besoin de la coopération des fournisseurs de logiciels et d'applications pour développer conjointement des solutions et des activités, comme par ex. OpenDNS/PhishTank comprenant les listes noires nécessaires.

5. PRIORITÉS POUR LES RÉGULATEURS

Les principaux fondements légaux de gestion des défis de la Confiance Numérique semblent largement mis en place, avec cependant une nécessité constante de réinterprétation des concepts régulateurs existants afin de prendre en compte les nouvelles technologies et les réalités du marché, du marketing et des usages. La nature transfrontalière des menaces envers la Confiance Numérique met particulièrement l'accent sur l'importance de la coopération internationale (judiciaire), de la prise de conscience accrue de l'urgence de l'action et, pour le gouvernement et les autorités exécutives, de l'affectation de ressources appropriées afin d'établir des structures efficaces de mitigation et des partenariats avec l'industrie. Il semble y avoir, dans la politique en général et dans les politiques de régulation, une tendance plutôt accentuée sur la coopération et la co-régulation des parties prenantes que sur l'activité législative – de fait, non seulement en Europe mais également aux Etats-Unis avec les mouvements récents de la FCC. En même temps, il est nécessaire de reconsidérer en permanence l'adéquation de toute activité régulatrice, notamment en cas d'approches fortement interventionnistes (telles que la « riposte graduée » ou les démarches visant à imposer un filtrage obligatoire du réseau) qui sont susceptibles d'empiéter sur les libertés fondamentales de l'Internet, sur les droits fondamentaux du consommateur (par ex. à la vie privée) et d'ébranler les certitudes légales acquises aux yeux des acteurs de l'industrie.

Les régulateurs doivent comprendre les rôles des opérateurs de réseaux/ FAI et l'impact d'une régulation potentielle sur ces rôles.

Dans d'autres cas tels que la mise en application d'exigences très strictes concernant la qualité du service, l'intervention régulatrice pourrait avoir des conséquences non souhaitées telles que l'entraînement de coûts considérables pour l'industrie en raison de mises à jour des réseaux. En conséquence, les régulateurs devraient mettre spécialement l'accent sur les interdépendances entre les différents domaines de la Confiance Numérique pour les différentes parties prenantes et équilibrer leurs décisions en conséquence.

Indubitablement, les régulateurs ont un rôle important à jouer pour garantir la Confiance Numérique. Étant donné la grande complexité des problèmes ayant une incidence sur la Confiance Numérique, le rôle des régulateurs visant à encourager une coopération accrue des parties prenantes pourrait être un moyen important pour parvenir à cette fin. Sur la base de l'analyse du présent rapport, les domaines suivants méritent l'attention continue des régulateurs :

L'implémentation de règles sans en considérer toutes les conséquences peut entraîner des pertes de revenus considérables pour toutes les parties prenantes.

• Encourager les opérateurs de réseaux et les FAI à mettre en place des politiques et procédures de la Confiance Numérique ainsi qu'une autorégulation basée sur des codes de conduite au niveau industriel – en particulier dans les domaines où une intervention plus importune serait susceptible d'entraîner des résultats économiques négatifs (par ex. la gestion du trafic) ou d'empiéter sur les droits fondamentaux des consommateurs (par ex. la règle « riposte graduée ou vous êtes dehors »).

• Considérer des mesures visant à limiter le risque juridique des opérateurs de réseaux et des FAI et, dans certains cas, le risque touchant leur réputation en introduisant des politiques et procédures de Confiance Numérique, par ex. mener le développement et encourager le déploiement dans toute l'industrie d'un registre de sites interdits dans l'intérêt de la protection des mineurs – et harmoniser en Europe les approches actuellement dispersées des différents pays, ceci incluant la mise en place de structures permettant des procédures coordonnées sur le plan international pour la protection des mineurs.

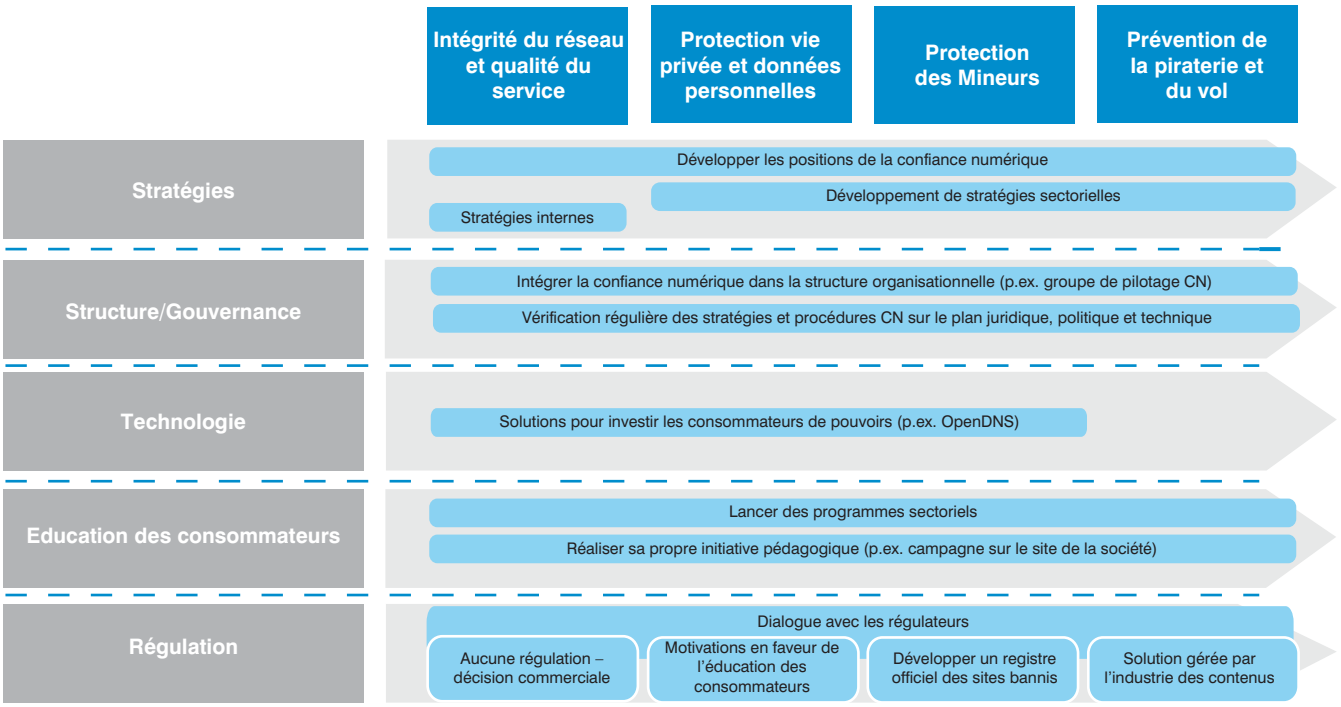
• Créer des stimulants pour les acteurs de l'industrie afin de leur faire adopter un rôle plus actif dans l'éducation des consommateurs – fournir des financements et mettre en place des initiatives de coordination pour un effet amplifié, par exemple en bâtissant sur les expériences acquises par le Programme pour un Internet plus Sûr.

• Accroître les efforts de coopération internationale pour développer des solutions globales ou des structures de résolution des problèmes globaux essentiels, par ex. dans le domaine de la protection des copyrights.

En résumé, la Confiance Numérique ne doit pas être nécessairement chère – en termes d'investissements requis – pour être réussie. Par contre, le coût de son échec serait substantiel. Cela dit, il n'est pas entièrement facile de faire fonctionner un programme de Confiance Numérique, et cela n'est pas entièrement gratuit non plus. La plupart des PDG qui affirment ceci sont de l'avis que leurs organisations s'impliquent dans un grand nombre d'activités parmi celles évoquées ci-dessus – à juste titre. Mais dans la majorité des cas, cela ne suffira pas. La Confiance Numérique dépasse largement le fait de mettre du matériel éducatif à disposition sur le site Web. Il s'agit de s'engager à un niveau supérieur avec les principales institutions privées ou publiques dans ce domaine et de lancer des campagnes sérieuses qui font la différence. Ceci nécessitera un financement et, le cas échéant, de nouvelles compétences dans les organisations. La Confiance Numérique ne se limite pas à la nécessité de posséder une politique de protection de la vie privée et des données sur fichier, il s'agit bien plus de changer la manière de penser d'une entreprise et sa manière de communiquer ces thèmes à ses clients et au public en général. En bref, la Confiance Numérique a besoin d'être menée par le haut afin de prévaloir.

L'importance du sujet est incontestée. Et il reste un long chemin à parcourir pour aborder toutes les problématiques, sans qu'il n'existe dans l'industrie du numérique aucune entité unique possédant toutes les réponses ou étant capable de résoudre à elle seule tous les problèmes. Il est nécessaire d'aborder la Confiance Numérique au niveau industriel, avec la participation active des principales parties prenantes suivant un cadre d'action commun et avec des rôles et des responsabilités clairs. De cette manière, la Confiance Numérique peut déployer tout son pouvoir et soutenir ainsi pour chacun les opportunités de création de valeur au sein des environnements numériques.

Illustration 62 : Priorités au sein des zones d'action



Note : CN = Confiance Numérique

AUTEURS DE L'ÉTUDE

Thomas Künstner
Vice Président
thomas.kuenstner@booz.com
+49 211 3890 143

Michael Fischer
Principal
michael.fischer@booz.com
+49 211 3890 168

John Ward
Associé Senior
john.ward@booz.com
+44 20 7393 3782

Martin F. Brunner
Associé Senior
martin.brunner@booz.com
+49 30 88705 842

Florian Pötscher
Consultant Senior
florian.poetscher@booz.com
+43 1 51822 900

BOOZ & COMPANY WORLDWIDE OFFICES

Asia

Beijing
Hong Kong
Seoul
Shanghai
Taipei
Tokyo

Australia, New Zealand, and Southeast Asia

Adelaide
Auckland
Bangkok
Brisbane
Canberra
Jakarta
Kuala Lumpur
Melbourne
Sydney

Europe

Amsterdam
Berlin
Copenhagen
Dublin
Düsseldorf
Frankfurt
Helsinki
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Rome
Stockholm
Stuttgart
Vienna
Warsaw
Zurich

Middle East

Abu Dhabi
Beirut
Cairo
Dubai
Riyadh

North America

Atlanta
Chicago
Cleveland
Dallas
Detroit
Florham Park
Houston
Los Angeles
McLean
Mexico City
New York City
Parsippany
San Francisco

South America

Buenos Aires
Rio de Janeiro
Santiago
São Paulo

09/08 Printed in Germany