IOL, pour Faire comme les Grands. LOL !

Publié le 25 septembre 2016 | par **Lurinas**

C'est un fait avéré, les données personnelles sont traquées, en masse, par les entreprises privées et les États. Pourtant, les révélations ne semblent pas émouvoir l'opinion publique, plongée dans ses smartphones et autres objets connectés, sitôt l'indignation évaporée. Aussi scandaleuses soient-elles. C'est à se demander si cela intéresse encore quelqu'un ? Si vous n'êtes pas cette personne, passez votre chemin, vous risqueriez d'apprendre que la France espionne massivement ses citoyens.

Trois ans déjà. En 2013, Snowden révélait l'existence du système de surveillance de masse de l'Internet mis en place par la NSA, l'agence gouvernementale américaine chargée de la sécurité intérieure, de quelques alliés (les Five Eyes) et **bien d'autres choses encore**. Comme un État de Droit en passe de devenir chaque jour un peu plus un État policier. Imperceptiblement. De façon bien indolore, par des **renonciations diffuses**.

Pire, nous y découvrions l'importance prise par les accords de coopération entre les agences de renseignement occidentales, lesquels prévoient des échanges massifs de données entre les services. Le GCHQ britannique ou le BND allemand collectaient les communications de résidents français en vertu de dispositions qui, dans leur droit national respectif, relèvent de la surveillance des communications internationales, puis les transféraient à leurs homologues français de la DGSE, afin d'échapper à tout encadrement et contrôle quant à l'utilisation de ces données. Une façon intelligente de contourner les maigres garanties applicables en matière de surveillance nationale.

Même pas mal

Mais c'est ainsi : le temps efface. Lave plus blanc que blanc. Le scandale a été remplacé par d'autres. **Ils se succèdent sans coup férir**. L'accumulation rend indigeste. Nausées puis vomissements, au début. Brefs. Puis histoire ancienne. Le corps est dorénavant immunisé contre les révélations de même ordre.

Cela va de soi maintenant qu'il est d'usage pour les grandes firmes mercantiles et lucratives du web (les GAFAM que sont Google, Amazon, FaceBook, Apple, Microsoft… pour les plus gros représentants d'entre toutes) de collecter et utiliser toutes les données de notre vie privée disponibles.

Mais cela a été un tout autre choc démocratique concernant ceux qui nous gouvernent. Un scandale mondial aux yeux de la population. Et étonnamment, c'est aujourd'hui à un ancien insider de prendre bonne mesure de la situation révélée. Ainsi , Michael Hayden, ancien directeur de la NSA et de la CIA (l'agence gouvernementale américaine chargée du renseignement extérieur) entre 1999 et 2009, explique que « d'une certaine manière, et de façon limitée, Snowden a été un cadeau. […] Il est la conséquence visible (mais pas la cause) d'un changement culturel majeur qui a redéfini la légitimité du secret, les nécessités de la transparence, et les fondements du consentement des gouvernés ».

Mais les choses sont revenues à leur équilibre habituel. Et l'Internet, devenu 'indispensable' dans notre quotidien, permet de mieux continuer à contrôler les citoyens. Imperceptiblement… La démultiplication des communications en échange d'un contrôle généralisé de nos données individuelles. Vice et versa. Par ces deux niveaux de surveillance.

Souriez, vous êtes surveillé

De partout donc ! Sans distinction, sans discontinuer.

Tout dernièrement, la Commission nationale de l'informatique et des libertés (CNIL) a mis en demeure le géant américain Microsoft de mettre son système d'exploitation Windows 10 en conformité avec la loi. Soit de cesser la collecte excessive de données et le suivi de la navigation des utilisateurs sans leur consentement, d'assurer de façon satisfaisante la sécurité et la confidentialité des données des utilisateurs et de renoncer à proposer des publicités ciblées, sans que le consentement n'ait été recueilli et/ou leur opposition possible.

Plus fraîchement, l'exemple de l'application populaire Pokemon Go est représentative des dérives et autres abus devenus tacites. Téléchargé plus de 100 millions de fois depuis son lancement en juillet dernier, ce jeu partage des données via le compte Gmail ou Facebook du joueur connecté sans que nul ne sache ce qui est fait de ces data.

On ne cesse de nous le démonter pourtant : les informations personnelles qui peuvent être déduites des seules métadonnées de ses appels et SMS (durée d'un appel, numéro appelé, heure de l'envoi d'un SMS…) sont très impressionnantes. C'est l'objet de la dernière **étude menée par l'université de Stanford** pendant plusieurs mois auprès de 823 participants (ils ont enregistré les métadonnées de plus de 250 000 appels et presque 1 250 000 SMS). Le nuage de ces data et les données de connexion laissées dans le sillage de l'internaute, prises

dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes (…) telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, leurs relations sociales et les milieux sociaux fréquentés, l'état de santé, l'ensemble des liens professionnels, les loisirs, mais aussi la vie sexuelle, les qualités, les défauts, les goûts, les engagements politiques, religieux, syndicaux…

Bref, des pans de vie très intimes qui mettent à nu celui qui pense s'abriter derrière le paravent de l'écran fêlé.

Des gardes-fous schizophréniques

Heureusement, les États veillent. Ils ont élaboré un vaste accord qui doit fixer les conditions minimales pour que des entreprises puissent transférer aux États-Unis les données personnelles de citoyens européens : le **Privacy Shield**. Il fait suite au Safe Harbor invalidé par la Cour de Justice de l'Union Européenne (CJUE) car permettant tacitement la surveillance massive exercée via les collectes de données des utilisateurs.

Certaines organisations non gouvernementales jugent cette refonte pourtant insuffisamment protectrice, les États-Unis s'engageant à ne pas pratiquer de surveillance excessive (sic) mais « sans fournir suffisamment de détails ».

D'un côté, la volonté gouvernementale de légiférer sur nos données personnelles. Tel le Privacy Shield donc, bouclier des données personnelles des citoyens Européens utilisées par les entreprises basées sur le sol américain. A toutes fins d'écarter la surveillance de masse non discriminée des données.

De l'autre, des États plus ou moins démocratiques attirés par la surveillance plus ou moins massive. De façon plus ou moins ciblée. Des États surveillants atteints de schizophrénie aiguë.

Et encore une fois, c'est un autre ponte de l'espionnage qui l'avoue. Lors d'une **conférence sise à Centrale-Supélec**. Bernard Barbier, l' ancien responsable technique de l'infrastructure d'écoute de la DGSE (le service de renseignement extérieur français) y confirmait que les États-Unis étaient derrière le piratage de l'Élysée, mais surtout y pointait l'action de la France dans une vaste campagne de cyber-espionnage.

De la récolte massive en France ?

On rigole, IOL !

Au moment où le gouvernement français s'offusquait d'un espionnage entre alliés et cependant que les révélations de Snowden terminaient de nous ébahir, la France collectait elle-même des données sur les backbones (des câbles sous-marins qui relient les côtes françaises à d'autres pays, voire à d'autres continents, par lesquels transitent 99 % des communications transcontinentales), avait un accord d'échanges d'informations avec les États-Unis (**projet Lustre**), vendait des systèmes d'écoute globale à des dictateurs et des États policiers. En toute discrétion. Secrets-défense et intérêts supérieurs de la nation mêlés. Pratique.

Et ces systèmes d'écoute globale, une obscure petite start-up française en maîtrise la conception et la maintenance. Cette technologie d'extraction des métadonnées, **Qosmos** en est le fer de lance français. Ce qui n'est pas sans passionner nos services secrets français attirés par le joujou.

> ***« Seule la technologie Qosmos fournit les applications en temps réel qui permettent d'identifier plus de 97 % du trafic et d'en extraire des métadonnées détaillées », selon l'entreprise***

Cet usage d'extraction a intéressé de beaux pays tels la Libye, selon l'emploi à double usage qui peut être fait de ces petits bijoux électroniques (double usage car pouvant être utilisés aussi bien dans le quotidien qu'en tant qu'armes). Ce qui n'est pas sans rendre intrigante la société Qosmos que les gouvernements successifs ne veulent pas laisser sans surveillance, justement, compte tenu de l' **intérêt stratégique qu'elle suscite** .

Oui, car contrairement à des armes explicitement militaires, ces produits manufacturés n'ont pas d'obligations de demande d'autorisation très contraignantes pour être exportés. Ce qui est pernicieux car le vendeur et l'acheteur savent pertinemment le double usage de ces technologies de cybersurveillance. Des produits dits à double usage très recherchés. C'est d'ailleurs pour cette raison que la **Commission européenne devait proposer des mesures** obligeant les entreprises à passer par de longues procédures d'approbation pour exporter les technologie biométriques, de géolocalisation ou de surveillance. Mesures finalement reportées par le président de la Commission, Junker. Allez savoir pourquoi…

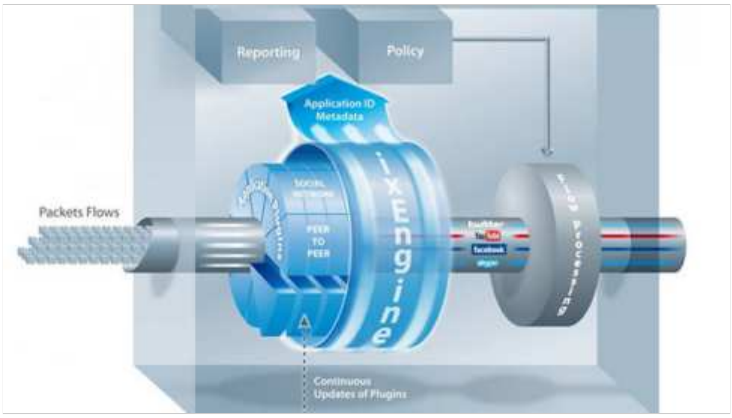
Ce double usage semble donc avoir également intéressé la France. Jusque-là, les lois portant sur la surveillance à l'étranger faisaient abstraction des conditions d'échanges de

renseignements, individuel ou massif (accords relatifs au partage ou aux accès aux dispositifs d'interception entre pays). Ouvrant possibilité de surveillance collatérale.

Bernard Barbier livre en toute exclusivité une ambition directe toute autre : la France aurait déjà effectué de la surveillance massive. Ce que ***Le Monde* dévoilait** furtivement à travers une note de Snowden en 2013, selon laquelle les services secrets canadiens suspectaient leurs homologues français d'être derrière une vaste campagne d'espionnage informatique débutée en 2009.

Tu parles d'une schizophrénie non bénigne. Ça frôle l **'hébéphrénie** . Ce programme existait donc! Dénommé IOL (pour Interceptions Obligations Légales), il consistait en l'installation et l'utilisation des sondes DPI (Deep Packet Inspection) au sein des **DSLAM** français (les équipements auxquels sont connectées les **fils de cuivre** des abonnés au téléphone pour accéder à l'Internet). Une mesure hors de tout cadre légal !

Mis au point entre 2005 et 2007, la généralisation à tous les opérateurs (soit 99% du trafic résidentiel) prévoyait l'installation de 'boites noires' sur les réseaux. L'outil décrit permettrait d'intercepter les communications électroniques d'un quartier, d'une ville, d'une région. Via des équipements d'analyse de trafic, les sondes DPI. Ce ne serait pas du systématique, comme le fait la NSA, mais une capacité d'interception assez conséquente. Du massif potentiel. En temps réel et de façon déportée. Dès 2009 !



Cette révélation éveille tout de même un débat entre experts, ne le cachons pas. Pour des raisons techniques pointues, qui de penser que **cette surveillance massive n'est pas possible** , **qui de valider cette faisabilité** .

Car en France, le réseau physique est extrêmement décentralisé. Le trafic n'emprunte donc pas systématiquement le cœur de réseau des opérateurs, mais circule en des multiples voies secondaires. L'installation sur tous les DSLAM s'avérerait donc pertinentes pour prétendre écouter tout ou partie du trafic à tout moment, mais demanderait des structures technologiques que d'aucun suppose inusitées dans notre pays.

Plusieurs ministres (dont celui de l'intérieur Cazeneuve) et députés devront certainement répondre de leur dénégation quant à l'utilisation des DPI en France. Donc bien loin des interceptions légales (**judiciaire ou administrative**) qui concernent une personne nominative.

> ***« Les sondes IOL et les boîtes noires fonctionnent exactement comme la reconnaissance faciale : elles sont obligées de capturer toute l'information qui passe pour en faire l'analyse. Et de la même manière que les caméras, ce n'est pas toute la population française qui est scannée, mais toute la population qui passe devant ces caméras. Ou toutes les métadonnées [voire] certaines informations contenues dans les paquets », dixit Kitetoa***

Il semble clair que de la collecte massive ait été testée en France. De quoi rompre le contrat social qui lie implicitement les citoyens aux représentants devant veiller à la préservation de la vie privée, aux respects des lois. Mais pour respecter les lois, il suffit tout simplement de les changer.

Légalisation a posteriori

Pour retomber sur son État de Droit, il est toujours temps de légaliser postérieurement.

Ainsi la pêche aux données en temps réel auprès des opérateurs n'a été rendue possible que par la **Loi de Programmation militaire** (LPM). Les autorités et les services parlaient alors des mesures antérieures comme ayant été « a-légales », des mesures en devenir, précurseurs, en avance sur leur temps… Alors qu'elles étaient tout bonnement illégales.

Même cause, même remède avec les lois **contre le terrorisme** (2014), sur le **Renseignement** (2015), sur la **surveillance des communications électroniques**

internationales (2015), sur la **réforme pénale** (2016). L'**état d'urgence renouvelé** et ses outils répressifs et/ou persuasifs sans cesse revisités. Toutes ont permis la légalisation de pratiques auparavant illégales. Plouf, plouf. A-légales…

La **loi sur le Renseignement** autorise le recueil en temps réel de l'ensemble des traces numériques (aspiration sur « sollicitation du réseau ») laissées dans le sillage d'une personne qualifiée de menaçante par les services par le truchement de « boites noires » justement. Ce qui n'est pas sans rappeler les fameuses sondes DPI posées sur les DSLAM… (retour ci-dessus)

Les dispositions sur la surveillance internationale légalisent également le vaste système de collecte du trafic de l'Internet mis en place par la DGSE depuis 2008 sur les backbones. Tous potentiellement espionnés sans discriminations (chouette, enfin l'égalité devant les institutions !). Mais le soupçon sans discernement n'est sans doute pas raisonnable.

Mais la société civile et les ONG veillent. **La Quadrature du Net** , **French Data Network FDN** et **Fédération des fournisseurs d'accès à Internet associatifs FFDN** , réunis au sein du collectif les '**Exégètes amateurs**', ont donc déposé un **recours auprès du Conseil d'État** contre la loi sur le Renseignement et ses décrets d'application, en usant de la jurisprudence de la CJUE. L'ensemble des arguments y sont développés.

Il faut dire que ces lois sont devenues alambiquées. Telle quelle, la loi sur le Renseignement autorise par exemple les services à espionner la population pour tout un tas de motifs (les intérêts majeurs de sa politique étrangère ; l'exécution de ses engagements européens et internationaux ; ses intérêts économiques, industriels et scientifiques majeurs ; la prévention de l'organisation de manifestation non déclarée ou ayant fait l'objet d'une déclaration incomplète ; la prévention de l'acquisition ou de l'emploi de stupéfiants à fins de consommation personnelle). Juridiquement, une loi aussi attentatoire doit pourtant présenter des finalités suffisamment « précises, strictement restreintes et susceptibles de justifier l'ingérence ».

Le diable se niche dans les détails

Plus exactement dans **l'article L811-5** , tiré d'un vieil article et utilisé à mauvais escient comme base d'un large système de surveillance.

> ***« les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre »***

Les voies hertziennes **concernent les informations transmises** :

- entre un téléphone portable et son antenne relai (GSM/3G/4G)
- entre une borne wifi et un ordinateur, un smartphone ou une tablette
- par un ordinateur portable utilisant une clé 3G/4G
- entre deux équipements Bluetooth (micros sans fil, etc.)
- entre un téléphone « sans fil » et sa base
- entre deux radioamateurs, deux talkie-walkie, etc.
- par des abonnés par satellite, WiMax, WiFi, etc.
- entre un badge de télépéage et la borne
- par une balise GPS
- entre une puce NFC/RFID (carte bleue, badge quelconque…) et sa borne.

Ces techniques « ne sont pas soumises aux dispositions » du livre VIII du code de la sécurité intérieur qui encadre toute l'activité de surveillance en France. Dès lors, la surveillance hertzienne est possible sans contrainte et pour quasiment tout support. C'est open bar ! Et les IMSI catchers, après les sondes DPI, de devenir les outils préférés des espions en herbe.

Avertir plutôt que guérir

Il n'est **pas trop tard pour se prémunir** . Et faire acte de résistance passive (*a minima*) pour perturber ces deux niveaux de surveillance (privé et étatique).

Culturellement et intrinsèquement, l'Internet est de nature décentrée. Et s'est donc imposé un nouveau modèle centralisé que de passer par Google pour toute recherche, d'utiliser les outils propriétaires du cloud de Microsoft, d'accéder aux vidéos via Youtube, de socialiser ses rapports sur Twitter ou Facebook… Cela crée des points de passage obligatoires, d'énormes silos de données, livrant ses données personnelles sans distinction à des acteurs oligopolistiques et rendant le contrôle des communications plus aisé.

La solution en cours de finalisation serait de retrouver décentralisation et/ou liberté par des outils opensource et collaboratifs. **Cela se nomme de façon caricaturale la 'dégooglisation'** .

Pour compléter, le visionnage de la **conférence « Reprendre sa vie numérique (et ses données) en main** » de Tristan Nitot (fondateur et ancien Président de Mozilla Europe et actuel Chief Product Officer de Cozy Cloud) est également instructive.

Ensuite, il s'agit de ne faire aucun obstacle à la cryptographie, équivalent numérique de l'enveloppe ou du carton qui préserve la confidentialité des échanges privés dans le monde physique. De tels outils de chiffrement semblent déplaire au ministre Cazeneuve puisqu'il souhaite en limiter son accès dans le cadre de la lutte contre le terrorisme : « Beaucoup des messages échangés en vue de la commission d'attentats terroristes le sont désormais par des moyens cryptés, ce qui rend difficile le travail des services de renseignement ». Il s'agirait « d'armer véritablement nos démocraties », rien de moins.

A écouter nos gouvernants technophiles, Telegram serait l'outil des terroristes, inventé par des russes qui plus est. A l'instar de l'Internet qui était (est encore ?) un nid de pédophiles et de nazillons. C'est oublier que **le chiffrement est indispensable** pour permettre le fonctionnement du commerce électronique et des banques. Il est aussi très important de le promouvoir pour limiter l'espionnage industriel (l'une des missions de la NSA et de nos services secrets).

La solution pourrait, après un ajustement temporaire des mœurs et des usages, résider dans une solution diamétralement opposée. **Laurent Chelma** reprenait l'idée du roman de John Brunner ('**Sur l'onde de choc** ', 1975) dans lequel un hacker qui, pour protéger ce qui reste de liberté dans son pays, finit par créer un virus qui va tout rendre public (toutes les données informatiques deviennent accessibles à tous au lieu de n'être possédées que par les institutions) ; il transforme ce faisant tout un monde, et fait plier un gouvernement corrompu. « Dès qu'il y a secret, où que ce soit, il y a possibilité pour le pouvoir de l'utiliser à son seul profit. […] A l'inverse, si je peux tout savoir sur tous, et que tous peuvent tout savoir de moi, alors […] plus personne ne s'intéressera à ma petite vie (ni moi aux leurs) et chacun pourra surveiller efficacement ceux qui ont du pouvoir sur nous ».

> ***Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes, selon l'article 12 de la Déclaration Universelle des Droits de l'Homme***

Avenir radieux…

Une société sous surveillance est le point de départ pour un État policier (relire impérativement « Surveiller et punir » de Michel Foucault). L'omni-surveillance instaure une prison dans l'esprit des gens, qui vont naturellement s'interdire de faire un certain nombre de choses. Oui, le problème ultime de la surveillance, c est qu'il change les comportements, de façon plus ou moins consciente. Le pas vers l auto-censure.

Compilées, triées, recoupées entre elles, ou même projetées dans des logiciels spécialisés qui en feront des cartes, dessins et autres graphiques, les données sont pernicieuses. Elles ouvrent horizon à une intelligence artificielle. Déjà, les experts utilisent des robots qui traquent des formules, expressions ou des profils identifiés. L'avenir nous rendra inévitablement dépendants d'algorithmes, avec son lot de décisions arbitraires, d'erreurs.

Depuis 2015, les services ont donc la capacité d'exploiter des algorithmes prédictifs, nourris de données de connexion aspirées sur les réseaux. Paramétrés, ces algorithmes veulent par traitements automatisés « **détecter des connexions susceptibles de révéler une menace terroriste** ». Des algorithmes prédictifs. Prévoir ensuite les déplacements, les centres d'intérêt, les préférences, voire le comportement, les choix, le rendement professionnel, la situation économique, l'état de santé… Vers une vocation transhumaniste que certains appellent de leurs vœux. Une route tracée pour l'algo-cratie, **l'algopolitique** …

> ***« Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre », disait le Cardinal Richelieu***

Or, dans le cas d'interceptions massives, où l'on recherche dans une masse de données des comportements « déviants », différents, ce n'est pas six lignes dont disposeraient les autorités, mais de milliards.

Notre problème n'est pas technologique, il est un choix social. Car entre les entreprises qui nous destinent à être des cibles publicitaires, les assurances qui nous pousseront aux comportements vertueux, les États qui nous obligeraient à l'autocensure, l'avenir s'annonce aussi radieux qu'une vie calibrée de fourmi.

Mise à jour (23 octobre 2016)

Le collectif des **Exégètes amateurs** a bien levé un lièvre. A tel point que le **Conseil Constitutionnel vient de leur donner raison** : le fait de procéder sans le moindre contrôle à la surveillance de communications par voie hertzienne (le fameux petit article **L811-5**, voir supra) est déclaré inconstitutionnel, en cela qu'il est contraire à l'article 2 de la Déclaration des droits de l'homme et du citoyen car portant *« une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances »*. En effet, cette disposition permettait aux services secrets de s'affranchir du code de procédure pénale qui encadre les écoutes ordonnées par un juge d'instruction.

La loi n'est pas pour autant abrogée mais le législateur se doit d'élaborer un nouveau texte d'ici le 31 décembre 2017 pour se mettre en conformité. Ce qui laisse encore quelques mois légalement consentis pour l'espionnage de masse. Nul doute que la refonte de cet article et de la loi sur le renseignement seront scrutés avec autant de persévérance.

Lurinas

Sources

Le dossier Qosmos and co. de Reflets.info

Mediapart

Postscriptum

Pendant ce temps-là, par voie référendaire, les Suisses approuvent par eux-mêmes, seuls, comme de bons adultes éclairés et informés, la loi **autorisant la surveillance des communications téléphoniques** et les activités sur Internet pour 'déjouer' les nouvelles menaces terroristes. Tant que les secrets bancaires ne sont pas inquiétés…

- **La NSA fait Beugler la Terre entière**

- **L'Acte Subversif de Manifestation Numérique**

- **[Hollandie] Panoptique, nous voilà !**
-

[Hollandie] Vous avez demandé la Loi sur le Renseignement, ne quittez pas

- **[Hollandie] Demain, Tous Suspects !**

Partager cet article

Twitter | Facebook | Envoyer

Les commentaires (1)

Frank | 26 septembre 2016 à 12 h 30 min

Excellent article.

À la une

- LaPrimaire.org
- Les Tziganes à l'Honneur
- Et Après ? La Douleur et la Fête
- Julien Letailleur 2017
- ÉLECTION USA VUE DE NEW YORK : TOUS LES REPORTAGES

Le meilleur

- SEMAINE DE LA PRESSE ET DES MÉDIAS À L'ÉCOLE : LE MONTEUR
- MUNICIPALES VUES PAR LA DROITE ET LA GAUCHE
- PUTES PRIDE 2008
- SAUVER KOKOPELLI ? MAMÈRE A UNE IDÉE…
- C'EST CLERC !

Journal

- Soutenez Melissa et Alexandre pour leur 4L Trophy !
- Délivrez l'Alerte !
- L'Art, pour Soigner nos Sociétés Malades
- [Ma Campagne Électorale] Dupont-Aignan
- IOL, pour Faire comme les Grands. LOL !

À propos

- Qui sommes-nous ?
- L'association
- Ils nous soutiennent
- Charte éditoriale
- Mentions légales
- Nous contacter

Culture Économie Médias Monde Politique Société Sport