

# Rôle stratégique de l'information dans les rapports de force entre acteurs économiques

L'information est devenue un enjeu géostratégique fondamental : elle structure les rapports de force économiques, politiques et médiatiques. À l'échelle mondiale, l'accès et le contrôle de l'information nourrissent la puissance des États et des multinationales, stimulent les manipulations géopolitiques et économiques, et creusent des inégalités numériques. Au niveau local en Belgique, la gestion de l'information façonne les rapports entre l'État, les entreprises, les syndicats, les médias et la société civile : transparence publique, usages numériques et conflits sociaux y redessinent les équilibres de pouvoir.

## 1. Au niveau mondial

### Accès à l'information et fractures numériques

Dans le monde, l'ampleur des inégalités d'accès à Internet est abyssale. Selon la Banque mondiale, **2,6 milliards de personnes n'ont toujours pas accès au réseau** <sup>1</sup>, principalement dans les pays en développement. Cette « fracture numérique » limite l'accès à l'information, creuse l'écart de développement (Nord/Sud) et confère un avantage aux puissances qui contrôlent les infrastructures (satellites, réseaux 5G, câbles sous-marins). Les États et entreprises les mieux outillés (câblage, télécommunications) fixent les conditions d'accès, par exemple en imposant leurs standards technologiques ou en restreignant les plateformes : c'est un rapport de force où l'information circule selon les intérêts des plus puissants. Les institutions internationales (ONU, Banque mondiale, OCDE) insistent sur la nécessité de combler ces lacunes – via l'ouverture de données publiques ou l'investissement dans le haut-débit – pour réduire les déséquilibres, car « la fracture numérique reste un enjeu mondial urgent » <sup>1</sup>.

### Désinformation et influence algorithmique

Les géants du Web (GAFAM, BATX) jouent un rôle central en façonnant l'information. Leurs algorithmes amplifient certaines données et opinions, souvent sans contrôle démocratique. L'OCDE souligne que la **désinformation massive** est une « menace grave » pour les sociétés modernes, sapant la confiance dans les institutions et la démocratie <sup>2</sup>. La Commission européenne met en garde : les campagnes étrangères de manipulation de l'information « constituent une menace grave » qui peut « fragiliser les institutions et les processus démocratiques » et « polariser la société » <sup>3</sup>. Mondialement, des États comme la Russie, la Chine ou d'autres utilisent propagande ciblée et fausses nouvelles pour influencer l'opinion publique (élections, guerre commerciale, crises sanitaires). Par exemple, la pandémie de COVID-19 a été marquée par une surabondance de fausses informations relayées par certains médias d'État ou réseaux sociaux, obligeant les gouvernements et ONG à contrebalancer par des campagnes de vérification.

Les plateformes elles-mêmes façonnent la perception du réel. Par leurs algorithmes, elles déterminent la visibilité des contenus (actualité, opinions, publicités politiques). Comme le notent les chercheurs d'ARC, les GAFAM « exercent une influence déterminante sur la façon même de penser et de modéliser (...) des choses plus politiquement fondamentales telles que l'État, les services publics, [ou] les idéologies gouvernementales » <sup>4</sup>. Autrement dit, les grandes entreprises numériques ne sont pas que

des censeurs privés: elles finissent par orienter le débat public et même la régulation du marché numérique <sup>5</sup>. Cette prééminence algorithmique renforce leur pouvoir économique et politique à l'échelle globale.

## Données, surveillance et souveraineté numérique

Au cœur des rapports de force économiques se trouve la propriété et la surveillance de l'information. Les flux de données (données personnelles, financières, industrielles) sont désormais un atout stratégique. Certains analystes parlent même de « colonialisme des données » : la collecte continue d'informations personnelles pour manipuler les comportements est présentée comme une nouvelle forme de domination, analogue à l'exploitation coloniale <sup>6</sup>. En pratique, les grandes puissances imposent leurs lois extra-territoriales pour capter ces informations stratégiques. Par exemple, les États-Unis se présentent comme un « Big Brother mondial des données économiques et commerciales » <sup>7</sup>. Christian Harbulot (CR451) rappelle que dans la « guerre économique » moderne, Washington utilise sa législation (FCPA, Sarbanes-Oxley, lois sur la concurrence) pour *“s'emparer [des] informations stratégiques”* des entreprises étrangères <sup>7</sup>, donnant aux régulateurs américains un accès aux comptes et données de multinationale du monde entier.

Par ailleurs, la surveillance de masse (cyberespionnage, Big data étatique) s'est généralisée. Les révélations Snowden (NSA) ou l'essor des technologies de reconnaissance faciale illustrent l'irruption de l'État dans les données personnelles. Les gouvernements cherchent à contrôler les flux numériques (5G, fournisseurs de cloud) pour des raisons de sécurité nationale, mais aussi de suprématie économique. Face à cela, plusieurs pays plaident pour une « souveraineté numérique »: maîtrise locale des infrastructures et données (Europe des données, circuits « cloud souverains ») afin de ne pas dépendre des géants étrangers. En parallèle, la réglementation internationale (RGPD en Europe, directives open data) tente de défendre la propriété citoyenne de certains types de données et de limiter les abus (transparence sur l'usage des données, droit à l'oubli). Le conflit technologique actuel entre les États-Unis et la Chine (sanctions sur Huawei, contrôle des puces, rivalités 5G/IA) illustre une guerre d'influence informationnelle où chaque camp multiplie les barrières pour protéger ses entreprises et savoir-faire.

## Exemples concrets à l'échelle mondiale

- **Manipulations électorales et guerres de l'information** : les réseaux sociaux ont été utilisés pour influencer des scrutins (référendum Brexit, élection US 2016 et suivantes) et pour polariser des sociétés. Les gouvernements renforcent la surveillance et la détection des faux contenus (lignes directrices de l'UE, fact-checking mondial).
- **Pandémie COVID et désinformation économique** : la crise sanitaire a déclenché une « infodémie » avec des vagues de fausses informations sur les vaccins ou les statistiques économiques, exploitées par certains gouvernements et entreprises pour favoriser leurs intérêts.
- **Cyberattaques et espionnage industriel** : des États (Chine, Russie, etc.) sont accusés de piratages massifs de données industrielles ou militaires (ex. usines, laboratoires pharmaceutiques) dans un cadre de guerre économique non déclarée.
- **Capitalisme de surveillance** : grandes plateformes technologiques (Google, Facebook, Amazon, Apple, etc.) collectent et monétisent des milliards de données humaines. Par leurs règles et algorithmes, elles orientent les marchés (publicité ciblée) et pressent les institutions à adopter leur vision du numérique (influence législative).

## 2. Au niveau local (Belgique)

### Transparence institutionnelle et données publiques

En Belgique, la question de la transparence et de l'accès aux données publiques a fait l'objet de réformes récentes. En juillet 2025, le gouvernement fédéral a approuvé une révision de la loi Open Data pour transposer une directive européenne. L'objectif est d'ouvrir largement les informations administratives : désormais la réutilisation des données publiques est « en principe gratuite », et les administrations doivent motiver tout refus <sup>8</sup>. Un « comité Open Data » a même été créé pour encourager la publication et la réutilisation des documents administratifs <sup>9</sup>. Cette démarche illustre la volonté d'utiliser l'information publique comme levier de croissance économique et de contrôle citoyen. Néanmoins, la confiance des Belges dans leurs institutions politiques reste très faible. Selon une enquête de l'IWEPS (Wallonie, 2023), à peine 22-39 % de la population fait confiance à l'État ou aux partis politiques (contre 78-87 % pour les secteurs santé/éducation) <sup>10</sup>. Ce faible capital de confiance (en chute d'environ 30 points depuis 2018) signifie que la transparence et la bonne gouvernance demeurent des enjeux clés : la mise à disposition de données officielles doit être accompagnée de garanties de qualité et de responsabilité pour restaurer la confiance démocratique.

### Médias publics et privés

Le paysage médiatique belge est marqué par sa division linguistique (flamand/valon) et par la présence de médias publics (VRT, RTBF) et privés (presse écrite, chaînes câblées, sites d'info). Un récent rapport du CRISP (sept. 2025) a d'ailleurs cartographié l'offre d'information en Belgique francophone, recensant presse écrite, audiovisuel et numérique <sup>11</sup>. Cette diversité survient pourtant sur un petit marché où la viabilité économique est précaire. Les médias jouent un rôle pivot dans les rapports de force locaux : ils peuvent soutenir tel projet économique (p. ex. grands groupes industriels) ou dévoiler des scandales, et sont souvent l'objet de polémiques sur le traitement de l'information (édition de « faits alternatifs », luttes d'influence). Par ailleurs, les réseaux sociaux sont devenus le terrain privilégié de la communication politique : lors des dernières élections (2024), les partis belges ont littéralement « saturé » la sphère numérique. Un rapport CRISP note qu'ils ont posté près de 25 000 messages et dépensé plus de 7 millions d'euros en publicité sur les réseaux sociaux <sup>12</sup> <sup>13</sup>. Tous les canaux – Facebook, Instagram, X/Twitter, TikTok, LinkedIn – ont été investis, souvent sans stratégie claire. Pourtant, comme le soulignent les analyses, cette frénésie numérique ne se traduit pas nécessairement par un gain électoral : « les likes et les partages ne se sont pas traduits dans les urnes » pour la plupart des partis <sup>14</sup>. Ces observations illustrent comment l'information (via les médias et plateformes sociales) est mobilisée en Belgique pour gagner en visibilité, même si l'effet concret sur le rapport de force politique reste parfois incertain.

### Conflits sociaux et vie privée au travail

Au niveau social, la numérisation a ravivé des contentieux entre syndicats et employeurs. Les syndicats belges veillent particulièrement aux droits à la vie privée des travailleurs. Un exemple emblématique est la CCT n°81, négociée fin 2017, qui encadre strictement la surveillance électronique en entreprise. Cette convention impose que tout système de contrôle des communications numériques soit justifié par des finalités claires (sécurité, lutte contre la fraude, etc.) et que les salariés soient informés préalablement de ces mesures <sup>15</sup> <sup>16</sup>. Elle exige en particulier la « transparence, proportionnalité et finalité » du contrôle <sup>15</sup>, et stipule que « les travailleurs doivent être informés à l'avance de tous les aspects du contrôle » <sup>16</sup>. Ce dispositif, fruit de négociations entre grandes entreprises et syndicats, illustre comment l'information (ici l'accès aux données de communication au travail) cristallise le rapport de force social : les syndicats obtiennent des garanties institutionnelles pour protéger les employés, freinant l'arbitraire patronal et toute surveillance excessive.

## Numérisation, données publiques et enjeux citoyens

Plus largement, la digitalisation de l'État et des services publics suscite des tensions. Le développement de l'e-gouvernement (services en ligne, identités numériques type eID) soulève des questions de sécurité et d'accès équitable. Par exemple, la cession de données biométriques aux forces de l'ordre ou la centralisation d'identités électroniques suscitent des débats sur la protection de la vie privée. En parallèle, la valorisation des *open data* (données publiques ouvertes) peut favoriser l'innovation (startups, chercheurs) mais oblige à garantir l'anonymisation et la qualité des informations fournies. Un autre enjeu local est la cybersécurité : la Belgique a créé en 2022 l'Agence de la sécurité de l'information (CERT.be) pour coordonner la sécurité numérique, reflet d'une préoccupation croissante face aux attaques informatiques transfrontalières.

Les organisations de la société civile (ONG, associations de consommateurs, think-tanks) jouent également un rôle : certaines fournissent des outils de veille citoyenne (sites de transparence politique, cartographie des firmes) ou font pression pour une gouvernance éthique du numérique (par exemple sur les thèmes de l'IA ou de l'évaluation environnementale des datas centers).

### Exemples concrets récents en Belgique

- **Données ouvertes** : en juillet 2025, la réforme Open Data a entériné la gratuité de principe pour la réutilisation des données publiques et renforcé les exigences de transparence (délai de réponse, motivation des refus) <sup>8</sup> <sup>9</sup>. Ce cadre vise à stimuler les innovations locales (applications mobiles, études urbaines) reposant sur les données de l'État fédéral et régional.
- **Cryptage et contrôle judiciaire** : la question du chiffrement des communications a fait la une (exemples : demandes des autorités d'accéder aux conversations cryptées). Le débat oppose la sécurité publique aux libertés numériques des citoyens, illustrant le rapport de force entre l'État et les grandes plateformes (ex. WhatsApp, Signal).
- **Fuite de données** : en décembre 2023, un cyberattaque contre Limburg.net (société de télécommunications régionale) a exposé les données de milliers de particuliers. Fin 2024, l'Autorité belge de protection des données (APD) enquêtait sur cet incident, soulignant l'importance accordée à la vie privée et la responsabilité des acteurs privés <sup>17</sup> <sup>18</sup>. L'APD rappelle qu'elle seule peut sanctionner les manquements au RGPD (le volet pénal étant du ressort du parquet) <sup>19</sup>.
- **Grèves et revendications numériques** : dans les services publics fédéraux et locaux, la diffusion de mails de grève (« statistiques » ou « capteurs » de grève) a suscité des polémiques récentes. Les syndicats ont demandé plus de transparence sur le traitement des données (par ex. qui compte les grévistes) afin d'éviter les manipulations. C'est un exemple où l'information – cette fois, les données sur la participation à une action sociale – est objet de conflit.
- **Présence politique en ligne** : lors des élections locales de 2024, certaines communes ont expérimenté des outils numériques de participation (e-votes, consultations en ligne). L'efficacité et la sécurité de ces outils ont fait débat, reflétant la méfiance des citoyens belges face aux promesses d'Internet.

En somme, en Belgique comme dans le monde, l'information se situe au cœur des rapports de force : elle est convoquée comme ressource par les puissants (pour influencer, vendre, contrôler) et défendue comme droit fondamental par les citoyens et institutions démocratiques. Les exemples ci-dessus illustrent l'importance stratégique de l'information – qu'il s'agisse de la rendre accessible (*open data*), de la protéger (vie privée, cybersécurité) ou de la déchiffrer (lutte contre la désinformation) – dans l'équilibre des pouvoirs économiques et sociaux.

1 Le Groupe de la Banque mondiale organise son deuxième Sommet mondial du numérique pour résorber la fracture digitale tout en stimulant la croissance économique  
<https://www.banquemondiale.org/fr/news/press-release/2025/03/18/world-bank-group-hosts-second-annual-global-digital-summit-to-bridge-the-digital-divide-and-boost-economic-growth>

2 Mésinformation et désinformation  
<https://www.oecd.org/fr/themes/mesinformation-et-desinformation.html>

3 Lutte contre la manipulation de l'information  
[https://commission.europa.eu/topics/countering-information-manipulation\\_fr](https://commission.europa.eu/topics/countering-information-manipulation_fr)

4 5 Les GAFAM et le pouvoir politique. Les algorithmes, représentants du peuple ? – ARC – Action et Recherche Culturelles  
<https://www.arc-culture.be/publications/les-gafam-et-le-pouvoir-politique-les-algorithmes-representants-du-peuple/>

6 Le colonialisme des données : repenser la relation entre le big data et le sujet contemporain  
<https://journals.openedition.org/questionsdecommunication/29845>

7 L'audit mondial sous surveillance américaine - CR451  
<https://cr451.fr/audit-mondial-sous-surveillance-americaine/>

8 9 Modifications concernant les données ouvertes et la réutilisation des informations du secteur public | News.belgium  
<https://news.belgium.be/fr/modifications-concernant-les-donnees-ouvertes-et-la-reutilisation-des-informations-du-secteur>

10 Confiance politique - Iweps  
<https://www.iweps.be/indicateur-statistique/confiance-politique/>

11 CRISP asbl | Centre de recherche et d'information socio-politiques  
<https://www.crisp.be/>

12 13 14 Réseaux sociaux et politique en Belgique (étude CRISP 2025)  
<https://www.xavierdegraux.be/reseaux-sociaux-et-politique-en-belgique-entre-communication-massive-et-engagement-uncertain-notre-étude-pour-le-crisp/>

15 16 Cct 81: Contrôle des données de communication électroniques en réseau | CGSLB  
<https://www.cgslb.be/fr/cct-81-controle-des-donnees-de-communication-electroniques-en-reseau>

17 18 19 Limburg.net: l'APD se penche sur l'aspect vie privée de cette fuite de données | Autorité de protection des données  
<https://www.autoriteprotectiondonnees.be/citoyen/actualites/2024/11/19/limburg.net-l-apd-se-penche-sur-l-aspect-vie-privee-de-cette-fuite-de-donnees>