Réseaux sociaux : le jumeau numérique qui s'attaque aux campagnes de désinformation

A partir d'une technologie qui permet de comprendre les pannes sur les grands réseaux électriques, une jeune société issue de recherches menées à Paris-Saclay a développé un modèle mathématique destiné à anticiper les campagnes de désinformation et de manipulation sur Internet qui sont décuplées par la multiplication de faux comptes pilotés par des IA.



Pour déjouer l'IA, Morphism fait appel à la modélisation mathématique. (Photo iStock)

Par Frank Niedercorn

Publié le 28 avr. 2026 à 10:40Mis à jour le 28 avr. 2026 à 11:08

Fin 2023, l'alerte aux punaises de lit a fait grand bruit quelques semaines avant le début des Jeux Olympiques de Paris 2024. Et pour cause, cette campagne de désinformation, dans laquelle la Russie a été impliquée, a été savamment organisée sur les réseaux sociaux grâce à des milliers de faux comptes. C'est contre ces manipulations de l'opinion qu'entend lutter la toute jeune société Morphism issue de recherches menées au Laboratoire interdisciplinaire des sciences du numérique (LISN) de l'Université Paris-Saclay.

Désinformation et réseaux sociaux font déjà bon ménage depuis une décennie sous l'effet de la multiplication des bots, ces faux comptes créés pour relayer la diffusion de fausses informations. Tout s'est accéléré avec l'avènement des intelligences artificielles génératives. « Sur les réseaux sociaux, on fait désormais face à une véritable ingénierie de la manipulation, coordonnée par des bots qu'il est quasiment impossible à détecter avec les techniques classiques de surveillance basées sur l'analyse sémantique des messages. Il faut changer de paradigme et tenter de comprendre comment se propage l'information afin de pouvoir anticiper ces attaques », explique Franck Rougeau, le cofondateur de Morphism.

Apprendre le mode opératoire des bots

Ainsi 37 % du trafic internet était dû en 2024 à des bots malveillants (contre 32 % en 2023), selon l'étude Bad Bot Report publiée en 2025 par Thales Cybersecurity qui notait que cette hausse se vérifiait « pour la sixième année consécutive ». L'IA générative permet de multiplier à l'envi ces bots mais surtout de les spécialiser. Certains pour liker des contenus, d'autres pour se connecter à certains comptes ou surtout relayer des messages de façon d'autant plus redoutable qu'ils sont à chaque fois modifiés, donnant l'illusion d'être émis par des êtres humains.

Pour déjouer l'IA, Morphism fait appel à la modélisation mathématique. « Nous créons une sorte de jumeau numérique des réseaux sociaux sur lesquels nous représentons la dynamique de propagation et non pas les messages, un peu comme Waze qui représente le trafic sans les véhicules. Nous détectons alors les anomalies de propagation pour identifier les bots et apprendre leur mode opératoire afin de pouvoir anticiper leurs actions », précise Franck Rougeau.

La technologie mise en oeuvre par Morphism repose sur les travaux de Bogdan Cautis, chercheur au LISN et spécialiste des graphes de diffusion. Cette discipline des mathématiques permet de modéliser la dynamique de propagation des pannes sur les réseaux électriques ou encore de mieux comprendre « l'évolution des crises d'épilepsie qui sont dues à une propagation virale de courts-circuits dans les neurones », précise Franck Rougeau.

L'ère des virus informationnels

La jeune entreprise a été créée en octobre 2025, avec l'ambition d'appliquer l'utilisation des graphes de diffusion aux réseaux sociaux. « Les points du graphe représentent les comptes dans les réseaux sociaux et les liens entre les points représentent la probabilité qu'une information passe d'un compte à l'autre », ajoute Franck Rougeau.

Morphism vient d'intégrer pour dix-huit mois IncubAlliance, l'incubateur deeptech de Paris-Saclay. Ses cofondateurs gardent des liens étroits avec la recherche académique, notamment le LISN (CentraleSupélec, CNRS, Université Paris-Saclay, Inria) et le Laboratoire d'informatique de Grenoble.

L'objectif est désormais de sortir un démonstrateur de la technologie, puis de lancer une première version du logiciel « testable en entreprise » d'ici la fin de l'année 2026. « Nous pensons que les bots sont en train de devenir un danger : de véritables virus informationnels au même titre que les virus informatiques et que les entreprises vont devoir s'en protéger avec des antibots comme elles le font avec des antivirus », prédit Franck Rougeau.

Frank Niedercorn