

Convergence des surveillances : l'effet des traitements algorithmiques agentiques

François Pellegrini

Professeur, Université de Bordeaux

francois.pellegrini@u-bordeaux.fr

Ce document est copiable et distribuable librement et gratuitement à la condition expresse que son contenu ne soit modifié en aucune façon, et en particulier que le nom de son auteur et de son institution d'origine continuent à y figurer, de même que le présent texte.

Grands modèles de langage (1)

- Les grands modèles de langage (GML) ont révolutionné la façon d'interagir avec les machines
 - Remplacement du formalisme strict des langues informatiques par le formalisme ambigu des langues humaines
 - Mais formalisme toujours...
 - Permet à un bien plus grand nombre de personnes d'interagir avec ces systèmes
 - Voire à l'ensemble de la population, avec les systèmes à interaction vocale

Grands modèles de langage (2)

- Ces systèmes sont extrêmement puissants et efficaces pour la production et l'analyse de textes
 - Notamment de codes sources
 - Développement de modèles spécialisés dédiés
- Capacité à corriger un texte sur la base de consignes spécifiées de façon plus ou moins formelles
 - Telles qu'un rapport de bogue avec reproducteur

Programmation « au ressenti »

- La spécialisation de certains modèles dans les langues informatique permet à des non-informaticiens de faire développer des logiciels complets de façon très rapide
- Programmation « au ressenti » (« *vibe-coding* »)
 - Le ressenti de l'utilisateur sert de guide pour orienter la production du système
 - Agir sur « les ombres » de l'interface permet de changer ce qui se trouve au fond de la « caverne » logicielle

Systèmes agentiques

- Les systèmes agentiques constituent une révolution supplémentaire dans l'interaction humain-machine
 - Distinction entre planification et exécution
 - Passage d'une interaction spécialisée du GML (action sur des systèmes bridés tels que des moteurs de recherche) à une interaction avec un ordinateur complet
 - Connecté à l'Internet
 - Permettent de (faire) construire et exécuter les outils nécessaires à l'exécution des tâches planifiées

Systèmes agentiques et collecte de DCP (1)

- Les GML actuels permettent de collecter et agréger des données ouvertes de sources multiples relatives aux personnes
 - Synthèses biographiques, etc.
- Les systèmes agentiques permettent à quiconque de construire des systèmes de collecte et de traitement massifs
 - Planification de la collecte et de l'agrégation
 - Facilité de fusion entre sources de données hétérogènes

Systemes agentiques et collecte de DCP (2)

- Les systèmes de surveillance, jadis conçus et mis en œuvre au sein des États et de sociétés spécialisées, sont désormais à la portée de tout un chacun
 - La programmation au ressenti permet de réaliser un logiciel de collecte et de surveillance de flux en deux semaines
 - Puissance de calcul disponible à la demande et à moindre coût

Systèmes agentiques et collecte de DCP (3)

- Disparition des garde-fous du temps de maturation et d'acquisition des connaissances en protection des données à caractère personnel
- Explosion des sources potentielles de violation de la loi « Informatique et Libertés »
 - Bien au-delà des habituels du secteur
- Facilitation des attaques de systèmes
 - Le système agentique met en œuvre les vecteurs d'attaque au profit de son usager
- Le « *script-kiddie* » devient un « *vibe-kiddie* »

Asymétrie informationnelle et libertés (1)

- La réduction de l'asymétrie de l'information sous-tend de nombreux droits et libertés
 - Liberté d'expression, liberté de la presse, droit à communication des documents administratifs, des pièces d'accusation, etc.
- Les grandes plateformes disposent d'un oligopole sur la capacité de traitement leur permettant d'exacerber cette asymétrie, y compris en matière de surveillance
 - Avantage matériel
 - Avantage cognitif

Asymétrie informationnelle et libertés (2)

- La mise à disposition généralisée des plateformes agentiques réduit cette asymétrie, mais amplifie le risque de surveillance

Systèmes agentiques et RIA

- Le Règlement « IA » (RIA) effectue une distinction selon les niveaux de risque supposés
 - Risques minimal, limité, haut, inacceptable
- Les « modèles de fondation » disposent d'un statut particulier, notamment ceux induisant un « risque systémique »
- Les systèmes agentiques ne sont-ils pas tous susceptibles d'appartenir à cette dernière catégorie ?