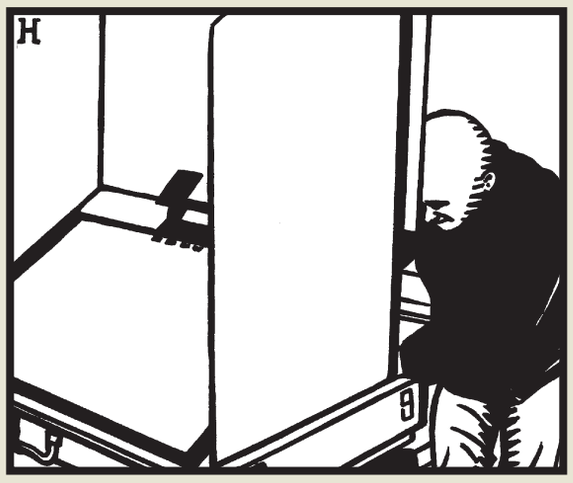
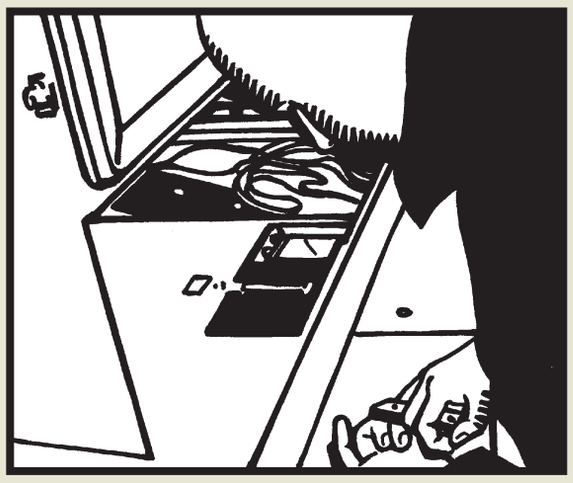
Un informaticien néerlandais vient de démontrer à quel point les ordinateurs de v

MACHINES À VOTER : RECETTE POUR

Comment pirater un ordinateur de vote



1 Ouvrir l'ordinateur de vote. À l'avant, des panneaux servent à cacher l'électeur aux regards indiscrets. À l'arrière, le cœur électronique comporte deux couvercles.



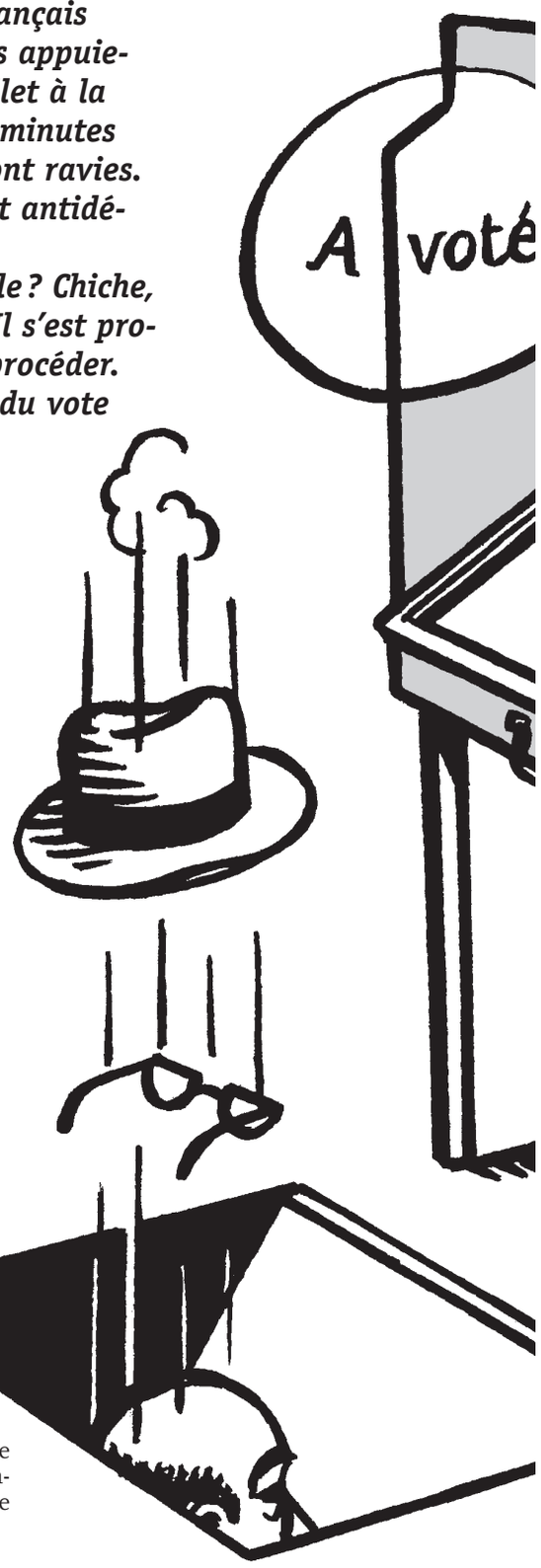
2 Sous l'un d'eux (à droite sur le dessin) se trouve la mémoire qui comptabilise les votes. Ce couvercle s'ouvre avec une clé standard, la même pour toutes les machines, et qu'on peut acheter sur Internet pour moins d'un euro. Ce qui est scandaleux, selon Rop : *« Par souci d'économie, ils n'ont pas voulu faire une serrure différente pour chaque machine. Ce qui montre que la procédure électorale n'est pas prise au sérieux. »*

3 Le couvercle de gauche s'ouvre avec un simple tournevis. Dessous, on accède aux circuits électroniques proprement dits.

4 Retirer un petit composant, qu'on appelle en langage informatique un « Eprom » pour « Ereasable Programmable Read Only Memory », autrement dit, « Mémoire programmable effaçable à lecture seule ». L'Eprom est une « vieille » technologie des années 1980.

5 Installer l'Eprom sur un appareil de lecture relié à un ordinateur (système en vente partout pour une centaine d'euros). Connaître le contenu de l'Eprom demande un peu de travail au début, mais rien d'insurmontable, à en croire Rop : *« N'importe quel bon informaticien peut faire ça. On passe un mois la première fois, puis, une fois qu'on a compris, c'est beaucoup plus rapide. »* Reprogrammer ensuite l'Eprom afin de favoriser le candidat désiré. Le remettre dans la machine à voter. Voilà, c'est fini. Personne ne remarquera la modification. **A. F.**

Pour la présidentielle de 2007, plus d'un million de Français voteront sur des ordinateurs. Fini le bulletin papier, ils appuieront sur une touche, un peu comme pour choisir un billet à la SNCF. Vu que le dépouillement ne prend que quelques minutes (un clic, une addition, c'est fini !), les municipalités sont ravies. Mais, pour bon nombre d'informaticiens, ce procédé est antidémocratique car il autorise une fraude indétectable. Impossible !, arguent les fabricants. Ah, bon, impossible ? Chiche, a répondu l'informaticien néerlandais Rop Gonggrijp. Il s'est procuré une machine à voter et nous a montré comment procéder. Cela, dans le but de stopper dans l'œuf la progression du vote électronique avant qu'il ne se répande en France.



Si je dis de Rop Gonggrijp qu'il est informaticien, vous allez imaginer un expert en blouse blanche. Si je le qualifie de fabricant de téléphones, vous pensez à obscur technicien. Si je le présente comme un hacker surdoué, c'est une sorte de boutonneux à lunettes qui apparaît. Et si je le traite de jeune militant politique alternatif, ça en fait un trublion anar. Rop Gonggrijp est un peu tout ça... et rien de tout ça.

Dans la maison d'Amsterdam où il me reçoit, une dizaine de jeunes s'affairent sur des ordinateurs *(voir encadré)*. Ambiance de boulot décontractée. Au mur, des affiches contre les machines à voter. L'une d'elles montre Staline surtitré d'une phrase qu'on lui attribue : *« Ce qui compte, ce n'est pas qui vote, mais qui compte les votes. »* Une autre paraphrase le film *Alien* en prévenant : *« Dans le cyberespace, personne ne vous entend voter. »*

Le Parti de la fraude toujours vainqueur

Rop qualifie son travail de *« recherche en sécurité »* et n'aime pas trop être qualifié de hacker : *« Hacker, cela fait hors-la-loi. Or, non seulement nous ne sommes pas contre la loi, mais, au contraire, nous en sommes de grands défenseurs. »* C'est tout le sens de son expérience sur les ordinateurs de vote (ou machines à voter). Les fabricants disent qu'ils sont fiables et qu'il est impossible de modifier leur programme. Qu'elles sont inviolables, en somme. Inviolables ? Eh bien, c'est ce qu'on va voir.

La première étape a été de se procurer des ordinateurs de vote. Pas facile, car ceux qui les vendent n'aiment pas qu'on mette le nez dans leurs affaires. Alors, Rop a grugé. Il a repéré des municipalités qui avaient des machines en trop, à cause de fusion de bureaux de vote. *« On leur a dit qu'on voulait leur acheter des machines pour organiser les élections du conseil d'entreprise de notre société. »*

C'est comme ça qu'ils ont déniché une machine de la marque Nedap. Pour nous, ça tombe bien. Ce fabricant néerlandais est précisément leader sur le marché français. Tout ce que nous dira Rop aura donc de bonnes chances d'être valable pour la majorité des ordinateurs de vote utilisés en France.

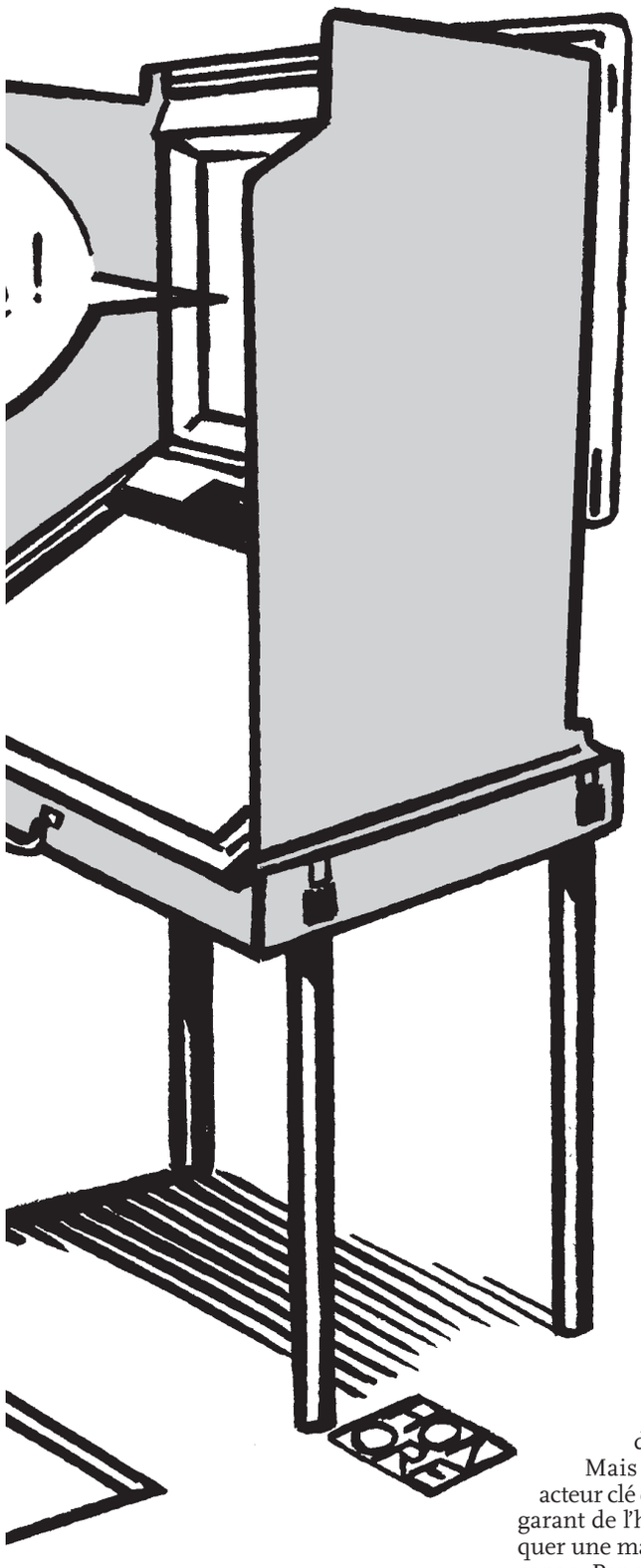
Le reste fut un jeu pour Rop : ouvrir le capot avec un tournevis, retirer le composant qui contient le programme, le modifier, puis le remettre dans l'ordinateur[1] *(voir encadré)*. Pour clore la démonstration, Rop me fait simuler une élection. Sur le panneau de l'ordinateur, une dizaine de candidats sont proposés. J'appuie plusieurs fois au hasard. À la fin, un rouleau de papier annonce le résultat du vote. Je découvre que le plus grand nombre de voix est obtenu par un parti (appelé malicieusement « Parti de la fraude ») pour lequel aucun des électeurs multiples que j'incarnais n'a voté. Normal : c'est précisément le parti que la petite manipulation de Rop avantage, quoi qu'il advienne. Une fraude parfaite, qu'aucun observateur de bureau de vote ne pourrait même soupçonner. « *Et ce que j'ai fait, n'importe quel programmateur de bon niveau peut le faire* », conclut Rop.

Des ordinateurs qui ne s'assument pas.

Dans la foulée, Rop montre aussi comment le secret de l'isoloir est aisément bafoué par les machines à voter. Il sort un simple récepteur de radiofréquences (vendu dans le commerce), et se place à quelques mètres de la machine sur laquelle nous continuons de simuler une élection... Et, surprise, le récepteur crépite différemment, selon le candidat choisi sur la machine à voter. Rien de mystérieux : car cette dernière envoie des ondes qui dépendent des touches actionnées. À peu de

ote (dont s'équipent plus d'une centaine de villes en France) sont faciles à pirater.

UNE FRAUDE ÉLECTORALE PARFAITE



frais, on pourrait donc connaître les tendances du vote en temps réel, et bien avant le dépouillement.

De retour en France, j'interroge évidemment Nedap. Je constate sur son site Internet que la marque (dont la branche française s'appelle France-Élections) a choisi le mépris en qualifiant l'expérience de Rop de « *soi-disant étude* » et, d'une manière générale, tous leurs détracteurs de gens qui « *pratiquent l'amalgame pour créer le sensationnel et la crainte* ». Pas vraiment sérieux, comme réponse. Pas beaucoup plus sérieux non plus, l'argument selon lequel leur machine ne serait pas un ordinateur car elle n'a ni écran, ni logiciel : « *Nos détracteurs l'accusent à tort d'être un ordinateur de vote* [pour] *lui attribuer les faiblesses de la micro-informatique* [...]. *Elle n'est pas attaquable ou piratable au moyen d'un programme et/ou d'un branchement avec ou sans fil dont elle ne dispose pas !!!* » (Les trois points d'exclamation sont de Nedap.)

On joue sur les mots en espérant rassurer le populo. Certes, les ordinateurs de vote n'ont pas de logiciel contenu dans un disque dur... Mais cela revient au même, puisque leur programme informatique est contenu dans des puces électroniques tout aussi piratables et modifiables ! Que Nedap se défende, c'est bien normal. Mais ça l'est moins de voir cet acteur clé du processus électoral, donc garant de l'honnêteté du scrutin, pratiquer une mauvaise foi qui frise le mensonge. Par exemple, quand Nedap écrit sur son site Internet, à propos des travaux de Rop, qu'« *à l'issue de sa recherche, ce groupe néerlandais a donc constaté que notre machine à voter fait exactement ce qu'on lui demande de faire* ». Oui, elle fait ce qu'on lui demande. Et il suffit justement de lui demander de tricher pour qu'elle le fasse sans rechigner (d'ailleurs, pour montrer à quel point la machine à voter est docile, Rop lui a même appris à jouer aux échecs...).

Hervé Palisson, directeur de France-Élections/Nedap, va jusqu'à nier les évidences : « *Les machines sont scellées. Pour les ouvrir, il faut un fer à souder.* » Il faut que je lui affirme avoir vu qu'il suffisait d'un tournevis pour lui faire abandonner cet argument. « *Oui, mais les machines sont sous surveillance. Les collectivités sont aussi honnêtes que nous, et tout est fait pour que la fraude ne soit pas possible. Et puis, vous vous rendez compte, il faut de nombreuses complicités et un informaticien.* » Eh oui, c'est justement le genre de choses qu'on trouve dans n'importe quelle municipalité. Quand on lui rétorque que l'existence des fraudes est aussi ancienne que celle des élections, Hervé Palisson ricane en vous classant dans les adeptes de « *la théorie du complot* ». Car « *la population doit avoir confiance dans les institutions* ». En gros, il n'y a pas de fraude parce que les gens sont honnêtes, et il n'est pas raisonnable de distiller le doute dans les esprits.

Une armée pour surveiller chaque machine

La fraude n'est évidemment pas propre au vote électronique. La question est de savoir si ce dernier la rend moins détectable que le vote traditionnel. J'ai bien l'impression que oui. Avec le papier, il faut supprimer ou substituer des milliers de bulletins. C'est compliqué, et on peut toujours les recompter pour voir s'il en manque. Avec le vote électronique, on change la puce, c'est quasi indétectable, et pour recompter, tintin.

Mais le pire n'est pas là. Dans une élection traditionnelle, pour limiter le risque de fraude, il suffit de surveiller les urnes le jour de l'élection (et quelques jours après s'il y a des litiges). Mais les ordinateurs de vote, c'est en permanence, à longueur d'année et vingt-quatre heures sur vingt-quatre, qu'il faut les surveiller, comme l'explique l'informaticien Pierre Muller[2] : « *On a beau mettre sous clé l'ordinateur de vote dans les jours qui précèdent les élections, la machine peut être piratée à tout moment, par exemple six mois ou un an avant le scrutin.* » Une telle surveillance étant quasi impossible, il suffit d'avoir la clé du local des ordinateurs et la complicité d'un informaticien, et hop, je t'embrouille. Ni traces, ni soupçon, ni contestation possible. De plus, poursuit Pierre Muller, «*les composants informatiques sont standards et programmés à l'identique sur toutes les machines. Il suffit d'en modifier un, de le dupliquer, d'en préparer un lot à l'avance qu'il suffirait d'installer dans les ordinateurs de vote et toutes les conditions sont réunies pour une fraude massive* ».

Pour une informatique éthique

Et puis, dans tout ça, il y a aussi une question de principe. Les élections, ça se doit d'être totalement transparent. C'est la base même de la démocratie. Or le contenu du programme intégré à l'ordinateur de vote est tenu secret par son fabricant. « *Si on le communique, on donne des informations à ceux qui voudraient frauder* », argumente Hervé Palisson.

En somme, l'honnêteté du scrutin repose sur la confiance qu'on attribue à une entreprise privée et commerciale. Ce qui, pour Rop, est parfaitement rétrograde : « *On appelle ça le principe de la "sécurité par l'obscurité" : si personne ne sait comment fonctionne le système, il ne peut pas être piraté. Mais l'ennui, c'est qu'il faut faire confiance au fabricant. Les gens de Nedap sont les derniers à défendre ce concept.* »

Il est réjouissant que l'opposition au vote électronique ne vienne pas de technophobes conservateurs, mais au contraire d'informaticiens à l'avant-garde des inventions. Quelle leçon, de les entendre faire l'apologie du bon vieux papier et reprocher à des élus ignares en informatique d'être « *victimes de la magie de la technologie* » !

Au fait, ça sert à quoi, le vote électronique ? Rapidité de dépouillement, économie de personnel, d'accord. En somme, tout ça pour gagner quatre ou cinq heures. Et qu'est-ce qu'on va en faire, de ces malheureuses heures ? Quand on les met en regard du risque de fraude indétectable, la balance avantages-inconvénients n'est assurément pas en faveur des ordinateurs de vote.

ANTONIO FISCHETTI

1. Publication de Rop Gonggrijp (en anglais) : www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
Des informaticiens de l'université Princeton ont fait le même genre d'expérience que Rop pour montrer la facilité de fraude sur les machines à voter américaines. Ils ont en tiré une publication et une vidéo : http://itpolicy.princeton.edu/voting/ts-paper.pdf

2. Pierre Muller est le fondateur et l'animateur du site www.ordinateurs-de-vote.org (où l'on trouve aussi l'article sur les machines à voter paru dans *Charlie* n° 736).

Le vote électronique en France

En France, on compte cent cinquante villes équipées — totalement ou partiellement — de machines à voter, ou en passe de l'être[1] : Bourges, Le Havre, Le Mans, Bagnolet, Orange, Brest, Reims, Boulogne-Billancourt... Au total, plus d'un million d'électeurs concernés (liste des villes sur le site de Pierre Muller).
Nedap est le premier fournisseur, avec quarante-cinq villes et huit cents bureaux de vote équipés. Mais les marques qui se partagent le reste du marché sont tout autant piratables que Nedap, à en croire Rop : « *Soit elles ont le même genre de composants électroniques, soit des composants encore plus faciles à modifier.* »
Les municipalités invoquent tous des gains de temps et de personnel pour le dépouillement. Afin de ne pas instruire qu'un procès à charge, il faut admettre les avantages du vote électronique : les votes nuls n'existent plus (car une touche correspond forcément à quelque chose — mais les votes blancs restent possibles), les petits candidats (qui ne peuvent s'offrir des bulletins papier dans tous les bureaux) peuvent être représentés, et les aveugles peuvent voter sans assistance.

Si on les titille un peu, les mairies se retranchent derrière l'homologation du ministère du l'Intérieur (« *On nous a dit que c'était fiable* »), lequel se retranche derrière l'agrément des labos d'inspection technique.
Ces derniers se contentent de vérifier que la machine calcule bien... Ce qui est la moindre des choses. Mais la question de la fraude potentielle n'est nullement envisagée... puisqu'elle n'est pas censée se produire !
Le cas de la ville de Grenoble est exemplaire. Car, après avoir envisagé de s'équiper en machines à voter, elle fait finalement marche arrière. Notamment grâce à Gilles Kuntz, adjoint au maire et maître de conférences en informatique, dont l'intervention mérite d'être largement citée : « *Cet important investissement, dont la rentabilité est loin d'être prouvée, pose de sérieux problèmes démocratiques. L'accès au code source de ces ordinateurs est impossible, même pour la Ville de Grenoble, qui désire les acquérir. Nul ne sait si les experts du ministère qui ont donné l'agrément de ces machines ont pu eux-mêmes examiner ce programme et prouver son exactitude et son inviolabilité.* » Il est significatif que l'une des premières villes à prendre conscience des risques du vote électronique soit Grenoble... ville qui a précisément fait des technosciences son image de marque.
Cela confirme ce que l'on disait plus haut à propos de Rop : les néophytes ont (parfois) davantage tendance à se laisser engluer dans une foi aveugle en la technologie (foi entretenue par les fabricants) que les spécialistes, plus à même de la démystifier et d'en cerner les dérives possibles.

A. F.

ROP GONGGRIJP, hacker autodidacte citoyen militant

À dix-huit ans, Rop arrête l'école et apprend l'informatique tout seul. Surdoué en la matière, il crée vite un groupe de hackers : « *Mais hacker dans le bon sens. Le but était de forcer l'accès au réseau pour tout le monde, alors que l'Internet n'était pas encore public.* » Déjà, la passion de l'informatique conjuguée à l'action militante. Parallèlement, Rop gagne sa vie en dirigeant une revue d'informatique, puis crée le premier fournisseur d'accès Internet aux Pays-Bas. Aujourd'hui, il dirige une petite entreprise qui fabrique des téléphones cryptés (c'est-à-dire impossibles à mettre sur écoute — pour une clientèle d'hommes d'affaires, par exemple).
Ça faisait longtemps que le vote électronique existait aux Pays-Bas, mais c'est quand la ville d'Amsterdam s'y est mise que Rop a réagi : « *C'est un grave danger si nos enfants grandissent en pensant qu'il est normal de ne pas être autorisé à connaître le fonctionnement des élections.* » Après avoir lancé le groupe « Nous ne faisons pas confiance aux ordinateurs de vote », c'est en octobre dernier qu'il décide de faire la preuve par l'expérience de la non-fiabilité des machines Nedap.
Il s'est ensuivi une énorme remise en question aux Pays-Bas : émissions de télé, création d'une commission nationale, mesures de surveillance renforcée des ordinateurs de vote, interdiction d'une autre marque de machines encore moins fiables que Nedap... Rop envisage maintenant de créer une coordination européenne des mouvements contre le vote électronique. **A. F.**

« Voter avec un ordinateur, cela revient à donner son bulletin de vote à quelqu'un qui dit qu'il va le remplir pour vous, sans pouvoir vérifier quoi que ce soit. »