

Editeur	Nom(s) solution(s)	Anonymisation de zone de texte ?	Anonym. De champs typés ?	Méthodes d'anonym. ?	Source(s) des données ?	Notes & commentaires (issus du site officiel)	Sources d'informations principales
(collaboratif)	Anonimatron	Non	Oui (une 20aine, possible d'en ajouter)	Une seule : synonymes (donc valeurs « réalistes »)	Bases de données (SGBDR, NoSQL) et fichiers structurés	- L'un des rares projet qui soit open source et libre (licence MIT), codé en Java. - Substitute les valeurs à masquer par d'autres valeurs de même type (et peut conserver le lien entre les deux valeurs si besoin, pour désanonymiser). Donc a priori il s'agit de substitutions bijectives et déterministes (une même valeur donnera toujours le même synonyme)	https://realrolfe.github.io/anonimatron/ https://realrolfe.github.io/anonimatron/documentation/
(collaboratif)	sdcMicro	Non	N/c	N/c	N/c	- Licence libre (GNU GPL v2), codé en R - Semble être un PoC universitaire	https://cran.r-project.org/web/packages/sdcMicro/index.html https://cran.r-project.org/web/packages/sdcMicro/sdcMicro.pdf
ARCAD Software	DOT Anonymizer	Oui	Oui	N/c	Bases de données, fichiers structurés	- Détection des données sensibles, cachées dans les champs commentaires - Utilise un moteur de règles - Masquage à la volée	https://arcadsoftware.fr/produits/dot-anonymizer-solution-multiplateforme-d-anon
ARX	Deidentifier	Non	Oui (> 10)	Plusieurs techniques	Bases de données (SGBDR, NoSQL) et fichiers structurés	- L'un des rares projet qui soit open source et libre (licence Apache), codé en Java. - Très bien documenté, en ligne (y compris publications scientifiques : https://arx.deidentifier.org/publications/) - Disponible sous forme d'un logiciel (multiplateformes) avec GUI, mais aussi sous forme de bibliothèque logicielle	https://arx.deidentifier.org/ https://arx.deidentifier.org/overview/ https://github.com/arx-deidentifier/arx
Athena Research Center	Amnesia	Non	Oui (pas de liste)	Plusieurs techniques (certaines personnalisables)	Fichiers structurés (type CSV, TCV ou XML)	- L'un des rares projet qui soit open source et libre (licence BSD), codé en Java. - Service accessible en ligne gratuitement : https://amnesia.openaire.eu/amnesia/	https://amnesia.openaire.eu/ https://github.com/dTsitsigkos/Amnesia
BlueTalon	Unifed Data Access Control (UDAC)	Non	N/c	N/c	Cloud uniquement ?	- Racheté par Microsoft en 2019	https://bluetalon.com/ https://bluetalon.com/product/
Broadcom	Test Data Management	Non	N/c	N/c	N/c	- Apparemment uniquement de l'anonymisation de champs typés - Broadcom étant principalement un fabricant de processeurs et dispositifs réseau, on peut se demander le but du rachat de CA Technologies.	https://www.broadcom.com/info/continuous-testing/test-data-management
CA Technologies	Test Data Manager for Masking and Subsetting	S/o	S/o	S/o	S/o	- CA Technologie a été rachetée par Broadcom en 2018. - Voir Broadcom	https://www.lemagit.fr/actualites/252444656/Mais-pourquoi-donc-Broadcom-rach
Camouflage Software Inc.	Datamasking	S/o	S/o	S/o	S/o	- Camouflage a été rachetée par Imperva Inc en 2017 - Voir Imperva	https://www.imperva.com/company/press_releases/imperva-acquires-data-secu
Compuware Corporation	Test Data Privacy	Non (voir note)	Oui	Plusieurs techniques, à base de « règles »	Mainframe, bases de données (SGBDR) et fichiers structurés	- "Traitement composé [qui] permet de localiser et d'anonymiser des morceaux de données à l'intérieur d'un champ plus large" mais en fait permet surtout de localiser un nom dans un champ contenant par exemple un nom complet.	https://www.compuware.com/fr/confidentialite-des-donnees-de-test/
Dataguise	DgSecure, DgDetect	Non	Oui	Plusieurs, à base de regex	Bases de données (SGBDR et NoSQL) et fichiers structurés	- Met en avant sa solution de découverte de données personnelles dans les sources de données "structurées, semi-structurées, non structurées", mais n'indique pas explicitement les zone de texte.	https://www.dataguise.com/general-data-protection-regulation-gdpr-compliance/ https://www.dataguise.com/detect/
Delphix Corp	Dynamic Data Platform / Axis	Non	Oui (30 types prédéfinis)	N/c	Bases de données (SGBDR et NoSQL) et fichiers structurés	- Solution de gouvernance de données globale (l'anonymisation en est une partie)	https://www.delphix.com/fr/platform https://www.delphix.com/fr/platform/masking https://www.delphix.com/sites/default/files/2018-10/PRINT_Datasheet_DataMas
Ekobit d.o.o.	BizDataX	Non	Oui (au moins 9 types prédéfinis)	Anonymisation avec données « réalistes » (même format/nature)	Bases de données (SGBDR)	- L'éditeur est surtout spécialisé dans le test d'application. - Aide à la découverte des données personnelles (y compris algorithmes heuristiques)	https://ekobit.com/our-work/bizdatax/ https://bizdatax.com/data-anonymization/ https://bizdatax.com/sensitive-data-discovery/
EPI-USE Labs	Data Secure	Non	Oui (env. 25 types prédéfinis)	Anonymisation avec données « réalistes » (même format/nature)	SAP essentiellement	- Spécialisé dans les systèmes SAP	https://www.epiuselabs.com/data-secure https://www.epiuselabs.com/secure-sensitive-sap-data https://www.epiuselabs.com/asset-delivery-masking-data-across-sap-and-non-s
GreenSQL	Dynamic Data Masking (DDM)	S/o	S/o	S/o	S/o	- La société n'existe plus (créée en 2009, issu d'un projet libre de 2007) - Le produit était un firewall SQL, qui avait quelques fonctionnalités pour anonymiser certaines données (dans les requêtes SQL) à la volée : hors sujet de ce comparatif (voir vidéo à 25:40)	http://greensql.com/ https://www.youtube.com/watch?v=ItdVUM81Svk
Grid-Tools	Datamaker	S/o	S/o	S/o	S/o	- Grid-Tools a été rachetée par CA Technologie en 2015, elle même rachetée par Broadcom en 2018. - Voir Broadcom	https://www.softwaretestingnews.co.uk/ca-technologies-acquires-grid-tools/
Hewlett Packard Enterprise (HPE)	SecureData Enterprise	Non	Oui (au moins numéros sociaux, ID, carte de crédit, compte, dates de naissance, salaires...)	Chiffrement et Format-Preserving Encryption (FPE) = valeurs « réalistes »	Base de données et fichiers structurés	- Solution globale pour la sécurité (issue du rachat de Voltage Security en 2015), dont une partie fait de la tokenisation / data masking. - Il s'agit plus d'une solution générique de chiffrement de données sensibles que d'une solution spécifique d'anonymisation (RGPD, données personnelles)	https://www.uk.sogeti.com/globalassets/uk/guides/hpe-securedata-enterprise.pdf
IBM	Guardium for Tokenization	Non	N/c	N/c	Bases de données (SGBDR et NoSQL) et fichiers structurés	- Système d'anonymisation à la volée de certaines données sensibles, qui donne accès soit aux données originales, soit à leur version masquées. - sorte de proxy générique pour accéder (via une application quelconque) indirectement aux données (en clair ou masquées selon profil).	https://www.ibm.com/fr-fr/marketplace/guardium-for-tokenization/details https://www.ibm.com/us-en/marketplace/guardium-for-tokenization
IBM	InfoSphere Optim Data Privacy / Data Masking	Non	Oui (pas de liste)	Plusieurs techniques (une 30aine, y compris valeurs « réalistes »)	Bases de données (SGBDR et NoSQL) et fichiers structurés	- Anonymisation en masse et à la volée - Très peu de documentation librement accessible	https://www.ibm.com/products/infosphere-optim-data-privacy https://www.ibm.com/downloads/cas/JGE5XOYY
Imperva	Camouflage Data Masking	Non	Oui (au moins 9 types prédéfinis)	Plusieurs techniques (y compris valeurs « réalistes »)	Bases de données (data warehouse et SGBDR) et fichiers structurés	- Apparemment uniquement de l'anonymisation de champs typés - Fonction d'aide à la localisation des données personnelles (en bases)	https://www.imperva.com/products/data-masking/ https://www.imperva.com/resources/datasheets/Imperva_Camouflage_Data_Ma

Editeur	Nom(s) solution(s)	Anonymisation de zone de texte ?	Anonym. De champs typés ?	Méthodes d'anonym. ?	Source(s) des données ?	Notes & commentaires (issus du site officiel)	Sources d'informations principales
Informatica	Dynamic Data Masking (DDM) et Persistent Data Masking (PDM)	Non	Oui (env. 11 types prédéfinis)	Plusieurs techniques (y compris valeurs « réalistes »)	Bases de données (data warehouse et SGBDR) et fichiers structurés	- 2 solutions : persistant (en masse, en base) ou Dynamic (à la volée) - Solution « Dynamic » : sorte de proxy générique pour accéder (via une application quelconque) indirectement aux données (en clair ou masquées selon profil).	https://www.informatica.com/fr/products/data-security/data-masking.html https://www.informatica.com/content/dam/informatica-com/en/collateral/data-shield https://docs.informatica.com/integration-cloud/cloud-data-integration/current-vers
Innovative Routines International, Inc (IRI)	Dark Shield	Oui	Oui (env. 14 types prédéfinis)	Plusieurs techniques (y compris valeurs « réalistes »)	Fichiers non structurés	- Indique savoir anonymiser les données non structurées (dark data : document, image, etc) - Utilise des RegEx prédéfinies, personnalisables, mais aussi « Natural Language Processing (NLP) and Machine Learning (ML) technology in DarkShield support Named Entity Recognition (NER) searches so you can find names, addresses, and other sensitive information in the context of your document formats. »	https://www.iri.com/products/darkshield/overview
Innovative Routines International, Inc (IRI)	Data Protector Suite	Non	Oui (env. 14 types prédéfinis)	Plusieurs techniques (y compris valeurs « réalistes »)	Bases de données (data warehouse, SGBDR, NoSQL) et fichiers structurés	- L'un des rares éditeurs commerciaux qui documente (avec copies d'écran) sa solution.	https://www.iri.com/products/iri-data-protector https://www.iri.com/blog/data-protection/classify-mask-pii-in-databases-with-field
K2View	TDM	Non	N/c	N/c	N/c	- Très peu d'informations accessibles sur l'anonymisation.	https://www.k2view.com/tdm-test-data-management/ https://www.k2view.com/data-as-a-service-fabric-technology/
Mentis Inc.	iMask	Non	Oui (quelques dizaines de types)	N/c	N/c	- Masquage statique et dynamique ? - Très peu de détail, discours commercial assez vague.	https://www.mentisinc.com/dynamic-data-masking/
Micro Focus	Voltage SecureData Enterprise	S/o	S/o	S/o	S/o	- Racheté (ou fusion ?) par HPE en 2017	https://www.microfocus.com/fr-fr/about/press-room/article/2017/micro-focus-com
National Library of Medicine (NLM)	NLM-Scrubber	Oui	Oui (pas de liste)	Une seule : substitution par nom du type de données	Fichiers ASCII uniquement (rapports médicaux)	- Logiciel gratuit (mais pas libre ou open source), gouvernemental, pour respecter la législation américaine HIPAA - Dédiée à l'anonymisation de données médicales - Après quelques tests : peu efficace, absences de détection de certains patronymes, les ages, les noms de maladies... - Le site indique que les données pourraient être désanonymisées par croisement avec d'autres sources (ils ont raison)	https://scrubber.nlm.nih.gov/
Net 2000 Ltd.	Data Masker	S/o	S/o	S/o	S/o	- Racheté par Redgate Software en 2017	https://www.realwire.com/releases/Redgate-adds-data-masking-solution-to-its-data-masking-portfolio http://www.net2000Ltd.com/DataMasker.html http://www.datamasker.com/
Oracle	Data Masking and Subsetting	Non	Oui (pas de liste)	Plusieurs techniques (y compris valeurs « réalistes »)	Base de données (SGBDR, NoSQL) et fichiers structurés (en masse et à la volée)	- Principalement pour bases Oracle, possible de transférer les données d'une base non Oracle vers une base Oracle avec une autre solution Oracle.	https://www.oracle.com/fr/security/anonymisation-data-masking.html https://www.oracle.com/database/technologies/security/data-masking-subsetting/ https://www.oracle.com/technetwork/database/options/data-masking-subsetting/
Privacy Analytics	Eclipse	Non	Oui (pas de liste)	Plusieurs techniques (y compris valeurs « réalistes »)	Oracle et SQL Server (uniquement ces 2 SGBDR) et fichiers structurés (CSV)	- Très peu d'informations accessibles sur l'anonymisation.	https://privacy-analytics.com/software/privacy-analytics-eclipse/ https://privacy-analytics.com/files/Why-Privacy-Analytics.pdf
Redgate	Data Masker	Non	Oui (pas de liste)	Plusieurs techniques (11 règles génériques + règles personnalisables, a priori aussi valeurs « réalistes »)	Oracle et SQL Server (uniquement ces 2 SGBDR)	- Le seul à indiquer un tarif : 7 800 dollars/an pour anonymiser 1To de données. - Documentations disponibles en ligne librement. - Peu de sources de données supportés (uniquement 2 SGBDR)	https://www.red-gate.com/products/dba/data-masker/ https://www.red-gate.com/products/dba/data-masker/resources/#documentation http://www.datamasker.com/DataMasking_WhatYouNeedToKnow.pdf
Solix Technologies	EDMS Data Masking	Non	Oui (pas de liste)	Plusieurs techniques (y compris valeurs « réalistes »)	Bases de données (data warehouse, SGBDR, NoSQL) et fichiers structurés	- Très peu d'informations accessibles sur l'anonymisation.	https://www.solix.com/data-management-solutions/data-masking/ https://www.solix.com/documents/datasheets/solix-edms-data-masking (2014)
Tata Consultancy Services (TCS)	DataPlus	Non	Oui (pas de liste)	N/c	N/c	- Très peu d'informations accessibles sur l'anonymisation.	https://mastercraft.tcs.com/Dataplus
Thales e-Security	Vormetric Dynamic Data Masking	Non	Oui (pas de liste)	Plusieurs techniques	Bases de données (data warehouse, SGBDR)	- Masquage dynamique (à la volée). Possibilité de traiter en masse avec « Batch Data Transformation » - Sorte de proxy générique pour accéder (via une application quelconque) indirectement aux données (en clair ou masquées selon profil).	https://www.thalesecurity.fr/products/vormetric-application-crypto-suite/tokenization https://go.thalesecurity.com/rs/480-LWA-970/images/ThalesEsecurity-Sb-tokenization
µ-Project team (collaboratif)	µ-Argus	Non	Oui (plusieurs dizaines)	Plusieurs techniques	A priori fichiers structurés	- Plus maintenu depuis début 2018 (manuel : 2014) : il semble qu'il s'agisse d'un PoC, issu d'un travail de recherche. - Licence non trouvée (non libre, mais apparemment open source), codé en Java	http://neon.vb.cbs.nl/casc/mu.htm http://neon.vb.cbs.nl/casc/Software/MUmanual5.1.3.pdf