

Vie privée

Comprendre qui nous observe

Cédric Lauradoux

INRIA

Présentation

- **Chargé de recherche INRIA (Privatics)**
 - ◇ membre du Grenoble Data Institute
 - ◇ membre de Cyber@Alps
 - ◇ Intervenant pour la Maison pour la science en Alpes-Dauphiné

Présentation

- **Chargé de recherche INRIA (Privatics)**

- ◇ membre du Grenoble Data Institute
- ◇ membre de Cyber@Alps
- ◇ Interveniant pour la Maison pour la science en Alpes-Dauphiné

- Auteur avec V. Roca et N. Bielova d'un

- MOOC sur la vie privée**

- <https://www.fun-mooc.fr/courses/course-v1:inria+41015+session03/about>

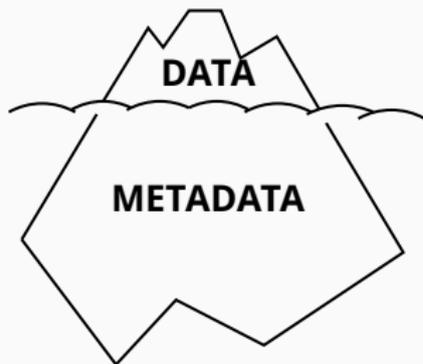
- `cedric.lauradoux@inria.fr`

Donnée et autres...

- Qu'est ce qu'une donnée ?
La qualification quantitative ou qualitative d'un sujet.

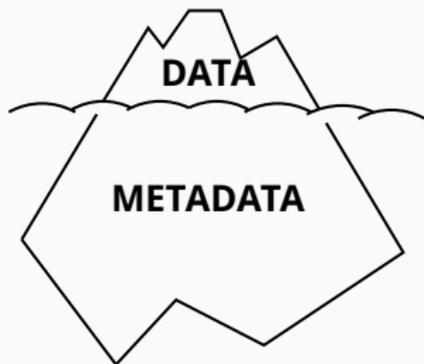
Donnée et autres...

- Qu'est ce qu'une donnée ?
La qualification quantitative ou qualitative d'un sujet.
- Métadonnée ?
Une donnée en décrivant une autre.



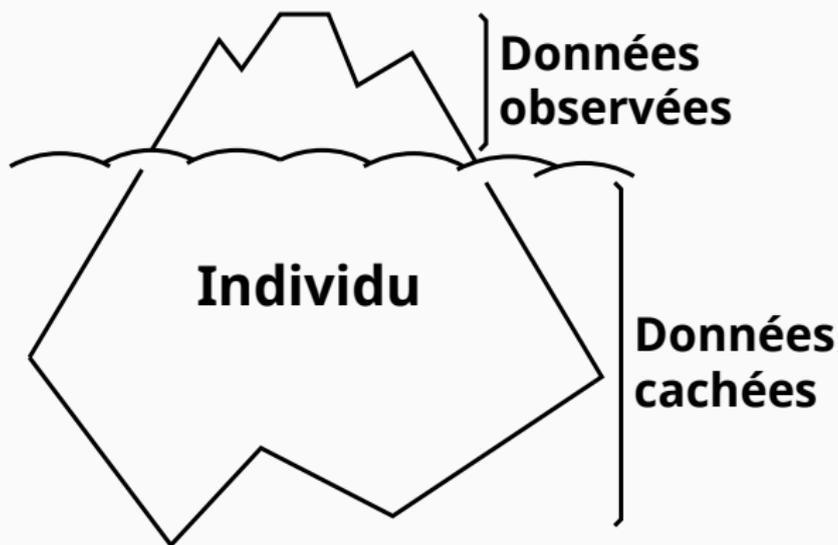
Donnée et autres...

- Qu'est ce qu'une donnée ?
La qualification quantitative ou qualitative d'un sujet.
- Métadonnée ?
Une donnée en décrivant une autre.



- Exemples ?

Qui exploite de nos données ?



- Données inférées ?

Données inférées

- Une donnée inférée est le résultat d'un **algorithme qui vous a observé.**

Cédric Lauradoux

2003-2007 INRIA Paris

2007-2008 Université de Princeton

2007-2008 Ami Reouven Elbaz-Vincent

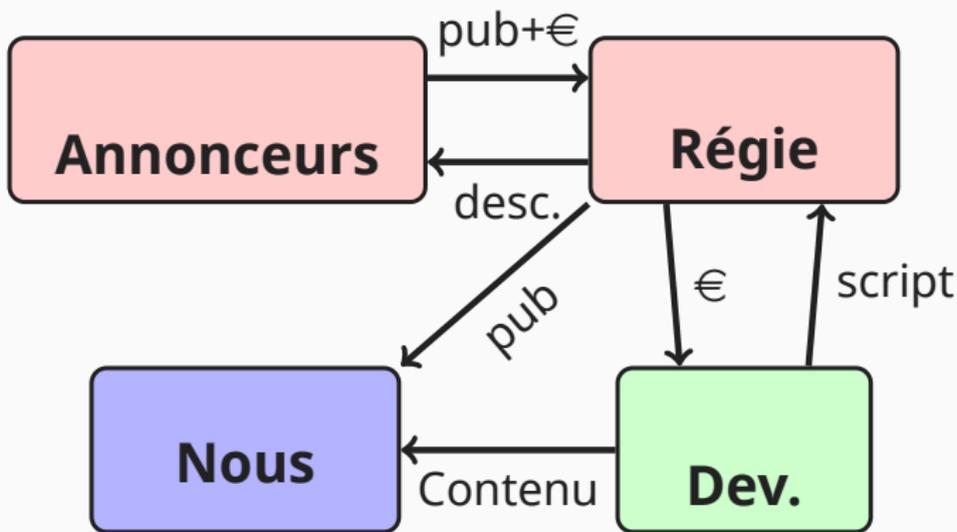
→ Cédric Lauradoux est juif.

- Le résultat est juste ou faux...
...mais vous allez le subir!

Qui s'intéresse à nos données ?

- Nous-mêmes (*quantified self*)
- La médecine (santé)
- L'État (recensement)
- Le marketing (publicité)
- Beaucoup de gens (futur employeur?)

Valeur de nos cookies



<https://ig.ft.com/how-much-is-your-personal-data-worth/>

Vous n'avez rien à cacher ?

- *“If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place”*

Eric Schmidt

- En 2004, CNET.com publie un biographie non-autorisée d'Eric Schmidt.
- Ils seront **blacklistés** par Google 1 an.

Hygiène numérique

- Ne pas être connecté est très radical...
Avoir un usage éclairé!
- **Contrôler son identité numérique:**
 - a. bien choisir ses identifiants,
 - b. bien choisir ses mots de passe,
 - c. contrôler ce qui est publié.

Choisir ces identifiants

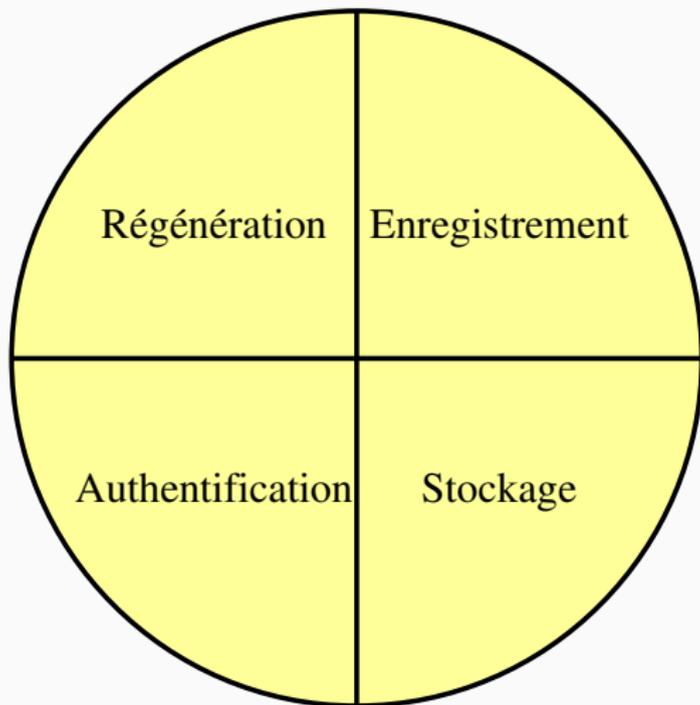
- **Comment choisir un identifiant ?**
 - a. j aime boire du lait
 - b. je deteste mes profs
- **Rester neutre !**
- **Ne rien divulguer:**
 - ◇ nom,
 - ◇ prénom,
 - ◇ localisation...

Divulguer son nom

(Dept. 26)



Mot de passe



Mot de passe

- Un mot de passe est une chaîne de caractères choisies **arbitrairement** par un être humain!
- *Souvent dans une conversation, on utilise le terme aléatoire à la place d'arbitraire.*
- Si un nombre aléatoire peut remplacer un nombre arbitraire, **l'inverse n'est pas vrai.**
- Votre mot de passe est connu de vous et de vous **seul** !

C'est quoi concrètement ?

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
001	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
002	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
003	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
004	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
005	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
006	'	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
007	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

- Lettres de l'alphabet (maj. et min.)
- Chiffres
- Caractères spéciaux

Comment le choisir ?

#	min.	min.+maj.	alphanum.	imprimable
3	10^4	10^5	10^5	10^6
4	10^5	10^6	10^7	10^7
5	10^7	10^8	10^9	10^{10}
6	10^8	10^{10}	10^{10}	10^{11}
7	10^9	10^{12}	10^{12}	10^{13}
8	10^{11}	10^{13}	10^{14}	10^{15}
14	10^{14}	10^{24}	10^{25}	10^{27}

Et la longueur ?

#	min.	min.+maj.	alphanum.	imprimable
3	10^4	10^5	10^5	10^6
4	10^5	10^6	10^7	10^7
5	10^7	10^8	10^9	10^{10}
6	10^8	10^{10}	10^{10}	10^{11}
7	10^9	10^{12}	10^{12}	10^{13}
8	10^{11}	10^{13}	10^{14}	10^{15}
14	10^{14}	10^{24}	10^{25}	10^{27}

- **ANSSI:** au moins 12 caractères !

Mais vraiment comment on choisit ?

- **Règles imposées à la création:**
 - ◇ *Majuscules/minuscules/chiffres/...,*
 - ◇ *Longueur.*
- **“Force du mot de passe”:**
 - ◇ *Échec = mot de passe faible*
 - ◇ *Succès ≠ mot de passe fort*
 - ◇ *Succès = accès au service*
- **Confiance relative donc.**
- <http://bit.ly/1eLPFQN>

Mot de passe	Fréquence
password	32027
123456	25969
12345678	8667
1234	5786
qwerty	5455
12345	4523
dragon	4321

- Humains = mots de passe simples.

Malgré tout ça...

- **La perte de vos données est inéluctable.**
- <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- <https://haveibeenpwned.com/>

Merci