Lesson 6 : Networked writing, Video 3.

Digital identity

18 juin 2015

Olivier Ertzscheid

Digital identity is the sum of all the information we leave on the Internet, whether willingly or unwillingly, and it is also the result of all this information as it will later appear, remixed and rearranged by search engines and social networks. You can see this, for example, when you type your name on Google, or look for your Facebook profile. Several types of information are collected. There is information that is more declarative in nature. When you join these sites, you fill in a profile form where you state your age, your place of birth, the high school you attended, and possibly even your political opinions too. Well, that is information over which you have some control. Then, there is all the information and data that are behavioural or content-related. This means that, each time you browse a website, information is collected that will be used to improve or add to the portrait that the site has of you. So there are these two broad categories of information. Well, this information is collected in different ways. First of all, within these sites themselves : each time that you interact on Facebook, for example, and each time that you chat with friends, all the information that you post on Facebook is directly harvested by Facebook. But also outside these sites : for example, when you are reading an article on the website of "Le Monde" and there is a "Like" sign at the end, and you click "Like", well, that piece of information will get back to Facebook and will add some data to your portrait, to the information that the website has about you. So awareness is necessary, it is important, and it is more and more the case, of course, in the context of school, but also at university. It is important because these are sites where the mechanisms are not as straightforward as they seem, and we have noticed over the past four or five years that awareness training is producing its first effects. That is to say that people are using these sites, these social networks, in a way that is less and less candid, and that they are more and more aware that there is in fact a public space, a semi-private space, and that whatever you may say on these sites will always run the risk, a very strong risk, of exposure, and you must be very careful quite simply with what you post, and the interactions you have with others. So, yes and no : there is a part that can be controlled. It is of course the part involving the information and data that we openly volunteer, what we say about ourselves. And then there is that other part, which by definition is much less controllable and which pertains to our interactions and behaviours. This includes all the sites we view, the history of our internet browsing, the log of our interactions on other sites, and also thanks to our "Likes" for example. This part is less easily controllable and is often where you can sometimes observe a certain amount of misuse, or perhaps blunders. Well, there are several types of misuse or blunders. For example, there is the type when you are looking for a job. In general, you are rather young, fresh out of university, it is true that you will often have a profile that is a student profile, where you have shared a number of funny, amusing, sometimes quirky things, which do not necessarily fit with what is expected of you in terms of professional identity. So that can be the first risk, even if employers are not supposed to check everything you did before you started to work for them. We know that most bosses, during job interviews, will automatically check the applicant's name on Google or Facebook, so you must be careful about that. Another risk, or misuse, is everything related to identity theft. For that there is a legal and judicial framework, making this a form of misuse that is already defined, against which protection exists, and so you can sue the perpetrator if you are a victim of identity theft. Well, then there is everything that is connected not so much to identity but rather to your e-reputation. Whether you are a company manager or a company employee, the way that you talk about your company will influence its reputation, the perceived image of the firm. So there too, you must be careful, and it is often complicated because with company managers, you are never sure if they are speaking for themselves or for their company, and the same goes for employees. Often you use the same account to share personal information and professional information, so you should try to compartmentalize these two areas a little bit more. The "Right to be Forgotten" has indeed been a work-in-progress for a rather long time, not only at the political level but also at the level of the National Data Protection Agencies (DPA, or CNIL in French). There have been attempts by the French CNIL, and then by the union of European DPAs, to enable citizens to assert their "Right to be Forgotten" by search engines and social networks. That means having the right to request the withdrawal of certain data, which we believe could be harmful to our reputation or our identity. In fact, it is very difficult to implement, since Facebook has 1.5 billion users and they log tens of millions of interactions every hour, so an enormous number of posts are published. Therefore it is only in cases where there is clear prejudice, if you are the victim of libel, or if you are insulted online, that it becomes fairly rapid and easy to have the information withdrawn. It nevertheless remains complicated to implement, inasmuch as we are dealing with platforms which are multinational, whereas the "Right to be Forgotten" pertains to national laws. It is therefore complex to ask these platforms to enforce such laws. Well, regarding good practices, there are several. The first, the basic rule is to regularly check the privacy settings of such sites, since it is those parameters that will define the perimeter of your digital identity, and it is the game plan of such platforms, especially Facebook, to reset their privacy settings every 6 months, or at least once a year, even when you had set them so as not to be too exposed. So that is the first point to check. It may also be interesting to think about registering or buying your domain name. Whether you are a student looking for job, for example, in order to post your CV online, or if you are a company manager, to protect a personal space of expression on the Internet. Well, when registering your domain name, and privacy settings, try to use tools wherever possible that are what we call open-source software programs, which will allow you to do the same thing. For example, there are open-source social networks, with the same features as Facebook, but within which you are not bound by the same general terms and conditions of use, which are very restrictive on Facebook, and according to which, once you have checked that little box (probably without reading the terms), all the information you post is available to Facebook, leaving you with very little control over anything. As soon as you are online, on Internet, whatever the platform you use, whether it is Facebook, Twitter, Google or something else, you are always in a public space. The notion of private space on the web or on the Internet does not exist. There are some chiaroscuro spaces, some spaces that are semi-private, but all the information you publish is always likely to end up in the public domain. So once you know that you are forearmed against most of the risks connected with this publishing activity. You must be careful what you publish, that is a key aspect. Not by self-censorship of course. You must simply be aware that, when you publish something on such sites, it will always reach an audience, and not necessarily the one you originally aimed to reach. So you need to have some sort of little cursor there, that is adapted to publication on social networks.