Digital Dilemmas Dialogue #9 | Transcript

Format: One-on-one moderated discussion
Length: 00h31m13s minutes
Date: 08.12.21

Mr. Staehelin
Good morning, good afternoon and good evening, and welcome to the 9th Digital Dilemmas Dialogue. My name is Balthasar Staehelin. I'm the ICRC Director of Digital Transformation and Data and I will be hosting this month's dialogue. We're going to be exploring an issue that is the subject of a full chapter in the *Handbook on Data Protection in Humanitarian Action*. As we're going to see this evening, there's still a lot to explore on this very important topic.

The topic we'll be discussing is the use of digital identity systems in humanitarian work. Those of you who have joined us for previous monthly DigitHarium sessions may be familiar with some of the problems that arise when creating permanent digital records for vulnerable people. In particular, during our discussions on biometrics, we kept returning to the dilemma of whether the benefits of introducing people into a stable support system that requires the creation of a digital identity outweigh the current and future risks of making those people more visible to actors and systems that may wish them harm. Of course, biometrics are by no means the only way of providing a digital identity, but they do create a framework and crystalize the tensions inherent to such systems.

The idea of using digital identities, particularly in the humanitarian sector, grew out of the need to provide people with a way to prove who they are and by extension that they belong to a certain category, such as citizens, aid beneficiaries, refugees, minors, etc. In most cases, humanitarian organizations need to know if someone fulfils certain criteria or ticks all the boxes in order to qualify for aid. For example, someone might need to prove their age to receive a vaccine. But that doesn't necessarily mean people need to be identified beyond their eligibility for a programme.

So there we have two problems that often come up in discussions of digital identity: imprecision, or the wide range of ways the concept can be interpreted, and the risk of voluntarily or involuntarily collecting more information than is needed for a given programme's aims. As we will see during this discussion, it may make more sense to talk about digital identities, plural, instead of the vague concept of digital identity in general. And if we want to use these new technologies responsibly, it's imperative that we think very carefully about the data we generate and collect and the best way to protect them.

To explore the issue and discuss a range of related topics, we're honoured to have with us today Professor Omar Seghrouchni, Chairman of the National Commission on Personal Data Protection, or CNDP as it's known in French, of the Kingdom of Morocco. Mr. Seghrouchni, thank you for joining us today.

Mr. Seghrouchni
Hello, thank you for having me.

Mr. Staehelin
Let me start with a question: what led you and the Commission to start thinking about digital identities? What are the most common questions you face about this issue?

Mr. Seghrouchni
We began working on it as a sort of historical accident. When we started examining this issue in 2018, we were being consulted as the competent authority on personal data protection. We were consulted regarding legislation that aimed to create a national register of the entire population, which reconfigured the issue of identity. We had to be very clear about potential issues with associating each person with a single identity and associating that identity with all sorts of biometric data. So we had to ask ourselves the question: is this approach proportionate, that is, proportionate to the stated objective. As you know, proportionality is a key principle in data protection, because we must always assess whether the game is worth the candle. In other words, are we seeking an overly complicated solution for a problem that might not be so complex as all that?

So that is how we ended up exploring a range of questions, and how we decided that the term "biometrics" is much too broad. Because biometrics includes fingerprints, iris recognition, facial recognition, and in the future it will include characteristics such as morphology, heartbeat readings, etc. In fact, there are three or four angles from which to consider digital identity: on the one hand, there are issues of authentication, and on the other, identification, which should really be considered as separate concepts, because authentication is one-on-one: I'm standing in front of you with a paper ID or a mechanism by which you identify me. Or "authenticate" me rather, whereas with identification I have a whole crowd of people and lots of information, which I use to pick out the identity of a given person.

The two processes are different, because biometric data do not play the same role in each. For example, if you want to prove your identity by putting your thumb on a fingerprint scanner, you're necessarily present, because you're the one touching the scanner. No one has cut off your thumb to use it elsewhere. You're also present when your iris is scanned. But with facial recognition systems, it isn't certain that you've consented to being identified in images from a security camera on the street. So there's the issue of consent that has to be dealt with. What governance measures can provide a framework for answering these questions?

So that's why this issue and the debate around it is so robust. We could spend hours talking about it, but in short, that's the answer to your question of how the Commission came to this issue. And the most common questions that arise concern proportionality, but also legality. So consent is not the only possible factor. We also have to consider what is in the public good, whether there's legitimate value, and also questions of legality. But can we make these two factors, legality and proportionality, correspond to our stated objective?

Mr. Staehelin
Thank you for that response. I'm reminded of what you said back in 2020: you stressed the importance of, and I quote: "avoiding the technically simplistic implementation of a single public identity, which can have unanticipated social and strategic consequences." You prefer a "segmented" digital identity concept. That's a very interesting idea. Can you tell us a bit more about

these types of identities and why segmentation is an important part of the best data protection solutions?

Mr. Seghrouchni

So we've been working on this, and we've come to the following conclusion: The end-goal is to be able to interlink different files so we can stay informed for matters of planning and public policy, such as if a given area needs more schools to be built. If the population is moving around within the country, some classrooms may be empty while others are overcrowded. So for matters of public policy planning, the utility is obvious.

In terms of humanitarian action also, which you mentioned just now, it can be important to know if a given person qualifies for benefits, for vaccination or a certain type of health care. So we need those files to be interlinked. What we've decided is, interlinking files, if it's done logically, if there's a legal framework and legal procedures to back it up, or even if it takes into account a State's foreign and domestic interests, that interlinkage is technically necessary. In simple terms, with a single identity, it's as if that interlinkage was permanent. We consider it important to have a single identity. It's good to have, but perhaps it should be kept on a technical level and not be made public to just anyone. What could be made public would be sector-specific, segmented identities that would reduce the risk that someone who knew you or your file might associate it with your tax information or create a simplistic link to your situation or your health status.

To be clear, in summary, if we were living in a perfect world where a single identity could be protected and its privacy ensured, where no one would be able to access it without authorization, there would be no problem with a single identity. So segmented or sector-specific identities are an extra level of security to protect a single identity, not to replace it. It's possible to meet our objectives using a single identity, if we stay within a legal framework, with sector-specific identities that protect against inappropriate use of that single identity.

Mr. Staehelin

Yes, in the humanitarian sector we're obviously thinking carefully about having a functional identity that would grant access to various services as opposed to a legal identity that aims to establish someone's exact identity. And we're trying to account for that difference in our service- delivery system and respect privacy and protect people's personal data. To return to digital identities in the humanitarian sector, as you mentioned, we often say how necessary it is to weigh the advantages of new digital technologies against the principle of "do no harm" which has been at the heart of our work in the humanitarian sector for decades vis a vis the people we are trying to protect and assist. Mr Seghrouchni, based on your experience in exploring the uses of digital identities, what are the main points of tension between digital identities and the protection and assistance that humanitarians seek to provide to people affected by armed conflict and other violence?

Mr. Seghrouchni

I'd like to make an analogy that I've been using recently, which might be a bit over-the-top. Think about a car. Just because your car's speedometer goes up to 220 km per hour, does that mean you

actually drive at 200 km per hour? Just because you need to get to your destination urgently and you're the only one who knows how urgent it is, you're the one saying how urgent it is, that doesn't mean you're allowed to drive any faster than 120 or 130 km per hour.

What I'm saying is, there's technology then there's how that technology is used. We're only allowed to drive up to 60 km per hour in urban areas for the simple reason that it lowers the risk of accidents in densely populated places. A speed limit of 120 or 130 km per hour on the motorway doesn't exist just for safety reasons, but also for environmental reasons, to limit consumption of petrol and carbon emissions.

So we need to distinguish between what technology makes possible and what society considers acceptable. That's why we generally say that we don't regulate technology, but the use of that technology. So, for humanitarian work, you have to weigh what is gained against what is lost. It may be more important to save a life than to consider issues of privacy. For example, during the pandemic response, I prioritized protecting the data of living people over the data of the deceased. Both are important but don't have the same urgency.

So in a sense, it comes back to the issue of proportionality that I mentioned earlier: putting things in context. The right to data protection is not the only right that exists. There's also the right to life, the right to work, etc. So we can't take only one factor into account. Each time, we have to consider the whole situation and multiple factors, but we can always allow something for a specific, limited timespan and decide to delete the data or delete the information that we had to collect to save a life. So again, it's the same issue as before: these problems cannot be tackled in absolute terms but have to be considered in context. And then, there have to be protection measures in place. One of which has to be, for cases where data had to be collected at a given time, not to share or use that data for anything but the stated objective for which it was collected.

Humanitarian action must not become a means of accumulating data that is then shared for other uses. What might happen if that data was shared with immigration authorities, for example? We have to think. I'm not saying there can't be a connection. I'm only saying that we have to step back and think through different scenarios and consider not just what technology makes possible, but how it's used.

Mr. Staehelin
Thank you for those points. I think you raise an absolutely fundamental question, and it reminds me that during the International Conference of the Red Cross and Red Crescent which includes States that are signatories of the Geneva Conventions, we adopted a resolution on the data collected while helping reunite missing people with their families, in which we were very insistent on the fact that that kind of humanitarian data should not be used for any other purpose. And it's indeed a fundamental point that you've raised, which is likely to stay relevant over the years to come, also in terms of building and sustaining people's trust in humanitarian organizations, so that trust is assured.

Perhaps we can dig deeper into that point, Mr Seghrouchni. During past discussions on biometric data we talked about how such data can be permanent and in some cases be preserved for decades. So those who generate and store such data have a degree of responsibility. What, in your view, are the data protection measures that must be in place, particularly regarding digital identities?

With regard to humanitarian organizations in particular, you shared that metaphor about not driving as fast as the car can go just because you can, and weighing various interests against each other, but in concrete terms, is there a point you'd like to make that we could continue to discuss at the roundtable in a few weeks? One that we could dig into deeper, that could help humanitarian organizations to assume full responsibility in these contexts given the vulnerable situation of the people we're working to assist?

Mr. Seghrouchni

Indeed. Thank you for asking that question because it gives me a chance to clarify, and clear up some fairly widespread confusion. Many people think of a single identity as being opposed to a sector-specific identity. But that's not the case. If we return to the idea of an identity specifically for the humanitarian sector: in fact, within the sphere of humanitarian action, that sector-specific identity is nothing less than a single identity for humanitarian aid. So whatever humanitarians want to do in terms of interlinking files can be done through a single, sector-specific identity. But since it's sector-specific, it can't be used for tax records or health records not related to humanitarian aid. So the sector-specific identity is a civilized, protected form of single identity. A single identity is a form of technical ID; a sector-specific identity is a social ID. And having a single identity for humanitarian aid is not a problem, so long as that identity cannot be used for anything outside of the humanitarian sector.

Mr. Staehelin

I think those are very important questions to be asking, and I'm sure there will be an impassioned debate about the impact of using a single identity in many of the contexts where our organization works. In some situations, there is no real State presence capable of providing a single identity.

So I think in unstructured situations like those, where the State is absent we're facing situations where the way in which humanitarians manage identities in order to provide aid poses real challenges. Especially when the aim is to find solutions that are fit for purpose and don't betray people's trust, and using digital technologies to create different identities. Legal identities, which are often created by the State, of course, to establish identity are very useful. There can also be functional identities that let us know if someone meets certain criteria, so that we can then provide a service without necessarily always having to know that person's legal identity. But I think this is an ongoing debate that will continue at the roundtable of experts we'll have in just under two weeks.

Perhaps if we could just zoom out a bit: you're tackling this issue because you're at the forefront of various debates on data protection, including on issues of digital identity, not just in Africa but I'd say globally. And I'd be interested to know what trends you've observed in those discussions, what trends are the most worrisome in countries engaged in this dialogue with regard to the technology that's available now? And what are the biggest advantages and opportunities? What is your impression of the state of the dialogue? And by that I mean beyond the humanitarian sector, as regards digital identities in general.

Mr. Seghrouchni
Well, I would say that we haven't yet achieved a mature level of dialogue. It seems to me we're still in the Wars of Religion, and we have to try to avoid a Massacre of Saint-Barthélemy. We're still at the stage of affirming our convictions, and I'm not sure that we've yet had a reasonable exchange of views given the camps that have formed. There's currently a deep divide between those touting the efficacy, utility, and ease of use of digital identities and those who maintain that digital identities can have undesirable consequences in terms of our values and fundamental liberties. There's the concept of proportionality that's upheld by various laws and regulatory authorities in charge of data protection. But that concept hasn't yet been widely recognized.

A certain type of data usage might be considered problematic under normal circumstances, but acceptable in a pandemic. We have to accept that there are no zero-risk situations, and that it's not a question of finding data solutions that are entirely without risk. That's not the issue. What we have to ask ourselves is: Are the risks that we're incurring reasonable compared to what we can gain? And once we've gained what we wanted, have we tolerated certain uses of data, and is there a way of checking that tolerance? Will we be able to delete what needs to be deleted, or will that data be reused for a different purpose?

So from my point of view, as I've said, I'm not complacent about these things. I applaud your initiative, because you're exploring possibilities that are timely and of importance to humanity, but at the same time, you're not entirely invested in one "religion" or the other: that's what we have to avoid. It's not single-identity-versus sector-specific-identity, it's what is the best combination? We at the CNDP use the term "identity architecture." The question isn't whether to choose one type of identity or identity, it's about creating an architecture that takes into account various situations, but is also adaptable over time.

Mr. Staehelin
What you say is very interesting because it makes me wonder if we haven't yet developed a common language to discuss this topic maturely. As you mentioned, with this series, Digital Dilemmas, we're trying to make a modest contribution to the debate in the context of humanitarian action, where these issues are crystalized in the extreme in terms of people's vulnerability, the risks they have to take. And the question remains: how can we be transparent about the risks people take as data subjects, as providers of personal data, and how we as humanitarians can model responsibility in that regard. Perhaps we can return to the roundtable discussions that will follow today's session. You talked about the need for dialogue, which often takes place between governments and humanitarian partners. Are there other types of professionals or experts who should be included in these debates to make them more effective?

Mr. Seghrouchni
I have always considered these questions not to be purely technical questions and that we need to include specialists in the social sciences, historians and various other specialists who contribute to our understanding of society. Human society isn't a machine, it isn't just a mass of data. Society is human beings, and interactions among human beings. So for me, this debate shouldn't be vertical, it should be as broad as possible.

Mr. Staehelin
Unfortunately, that's all the time we have. It's been a pleasure to have with us Professor Omar Seghrouchni, Chairman of the National Commission on Personal Data Protection, or CNDP, of the Kingdom of Morocco. Thank you so much for joining us today.

Mr. Seghrouchni
Thanks again for this initiative and for inviting me to speak.

Mr. Staehelin
Goodbye.

Mr. Seghrouchni
Goodbye.