NJORD Estonia: A free application can be expensive

As time spent on the web and on devices grows exponentially, the importance of the data sent and exchanged there becomes even more important as a currency.

Banks do not allow free access to their databases or to the treasury, others have to follow the same principle: companies dealing with their employees' and customers' data and confidential business and production secrets, doctors with patient treatment data and educational institutions upon using technology solutions for studies.

If the school recommends a platform on which the student must create an account or download something, the school must know if the user terms of this e-service provider allow users of a certain age to use the application, what data the downloaded application is collecting from the user, ie the student's and teacher's computer, and where it is transmitted.

The Estonian people and institutions have been proficient computer users for decades, but they still tend to forget that a free application is never quite free. Access to our data (how long we use different applications, what we download and upload, what we transmit, where we click, where we store data and how many contacts we have) has a comparable monetary value and is resold to other parties we usually have no idea about.

On the one hand, we can well ignore the resale of data, because at first glance it gets out of our control anyway, but on the other hand, we must be prepared for compromising conversations, as images and videos get accessed by people with whom we would not want to share them.

Secure and insecure channels

The ongoing crisis is the icing on a cake for IT services and product developers. The state is facing several challenges by having to create additional practical functions in a number of public services, especially in the field of e-health, and also make changes to the existing legislation if necessary. It is logical to assume that the general practitioners burdened with their daily work do not have to switch between the various electronic communication channels, mostly chosen by patients, to help their patients and also to monitor all kinds of privacy policies.

However, as a professional service provider, the GP should inform the patients about the risks involved in transmitting sensitive personal data through random channels. To reduce this workload, eHealth solutions should provide a secure channel of communication between the doctor, the nurse and the patient, where these parties can exchange information in one place. And that there would actually be a place where to direct people and where the communication between the doctor and the patient would be maintained.

Currently, the doctor communicates with the patient via e-mail or communication software, gives recommendations, etc., and then makes the corresponding entries in the electronic health information system. This is a duplication of work. In addition, e-mails and chat platforms in different applications do not have secure authentication or identification process which exists on the national e-health patient portal. The risk of actually treating another person through the patient must be minimized.

E-health service and e-learning have come to stay. Both public and private e-services can be provided in case the necessary infrastructure is available for both, the service provider and the service recipient. Who will bear the costs and to what extent, in order to create this infrastructure, is open to public debate. How much and how often should those be helped who cannot afford to buy the necessary resources? How to help families with several school children who need to attend different classes at the same time and need separate devices and quiet space to take part in the work of the e-classroom?

The courses have been prepared for classical teaching and e-learning was not familiar to all schools and teachers. At present, teachers, students, and parents are working hard to find the right methodologies and balance for e-learning. However, future courses must support the new form of study and the organizational and private infrastructure must catch up with the new challenges.

Incompetent e-shops

Surprisingly, it should be noted that larger and smaller merchants are not familiar with the charms and pains of e-commerce and are only now discovering shortcomings in their services or are just starting to think about the concept of e-commerce in a hurry. In good times, our larger retail chains have behaved similarly to large countries, which do not consider digitalisation to be vital because the money comes in anyway and every penny doesn't seem to be worth picking up.

If the average shopper chooses his most visited grocery store for logistical reasons, then now new factors arise with e-shopping. ie whether this e-shop exists at all, how it visually looks on the screen, how convenient it is to find items, whether and how solutions to your concerns are offered. It is also important to find out if the helpline is working and how long the queue is, when and how the goods will be received, how problems with the shipment will be resolved and how the privacy policy and terms of use are formulated.

The incompetence of the e-shop in technical compliance and organizational confusion, hidden from the customers, is in any case passed on to the customers and a new e-shop will be found with a few mouse clicks. Small producers, who have so far been able to sell the thrill and lifestyle that comes with their main product, cannot escape either. If the buyer has to make additional efforts to get a more expensive eco-lemonade that disappears with a couple of sips, then the manufacturer will not receive a second order from the customer.

If the sceptics of teleworking and distant learning undergo a change of mentality during this crisis, they must have the option to adopt integral solutions supporting their work. The keywords must be security, user-friendliness, functionality and user support. Incomplete e-solutions cost time and nerves.

There will be more resentment from customers and employees and it's a ticking bomb into scandals when things start to happen with insecure data that we cannot predict even in our worst dreams today. The advent of data crises is only a matter of time.

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE