

# The Characteristics Electronic and Digital Evidences in Saudi Arabia

**Lina Samaha** - Senior Associate - Dispute Resolution

l.samaha@tamimi.com - Jeddah

Developments currently occurring in Saudi Arabia's legal system include the issuing of coded laws in various legal areas to decrease the independence on Shari'ah law (which is not coded). Consequently, it has become necessary to also develop the judicial system to comply with the needs of today's digital world, including the anticipated heavier reliance on digital and electronic evidence. As many interactions now take place in the virtual world, recent Saudi laws have been issued to provide a framework for the submission of electronic or digital evidence, which will permit parties to enter into evidence documents that do not exist in physical form.

Up until recently, there was no coded law of evidence in Saudi Arabia and, therefore, such topic was discussed in multiple legislations, including the Law of Civil Procedures, Commercial Courts Law, and their Executive Regulations. In December 2021, a law of evidence was codified in Saudi Arabia (issued by the Board of Ministers Resolution no. 283 dated 24/05/1443H, corresponding to 28 December 2021) which shall enter into force on 23 June 2022 (the '**Law of Evidence**'). This law cancels and replaces the chapters discussing evidence in the aforementioned multiple laws and regulations, as well as efficiently codifies the provisions relating to evidence and their submission before Courts.

Considering fast and vast developments in today's world and the heavier reliance on technology and digital means, the Saudi Ministry of Justice, before the issuance of the Law of Evidence, shed light on the importance of digital and electronic evidence. Therefore, the Saudi Supreme Court issued its Resolution no. 34 dated 24/04/1439, corresponding to 11<sup>th</sup> January 2018 (the '**Resolution**') regarding the admissibility of digital proof as an evidentiary tool. The Resolution provides that a digital evidence shall be considered an evidentiary tool or proof as long as it is clear from any doubt; however, its enforceability as an evidentiary tool differs depending on the case and its facts.

The Law of Evidence defines a 'digital evidence' as any evidence derived from any data that is generated, issued, delivered, preserved, or communicated by digital means, and is retrieval or obtainable in an understandable manner. As per the Law of Evidence, a digital or electronic evidence shall have the power of a written (or physical) evidence.

Digital and electronic evidence would logically either be created by public authorities or private persons. However, when such digital or electronic evidence, that is presented to the Court, is not created by a public authority, it would be considered an evidentiary tool by the judge only in three occasions, as following:

1. if it was created in accordance with the Personal Data Protection Law and the E-Commerce Law;\*
2. if it was derived from a digital means that is mentioned in the agreement from which the dispute is arising; and
3. if it was derived from a digital means that is authenticated or can be used by the general public (i.e. an electronic platform that is available to the general public).

\*we do not address the E-Commerce Law in this article considering its technical nature.

Considering the above, it is worthy to discuss the Personal Data Law and the relevant conditions that the Court would look into in order to determine whether to accept a digital or electronic evidence that includes personal data. The Personal Data Law defines 'personal data' as every statement -whatever its source or form- that would lead to a specific person being identified, or make it possible to identify him directly or

indirectly, including: name, personal identification number, addresses, contact numbers, licence numbers, records and personal property, bank account and credit card numbers, still or moving photos of the individual, and other data of a personal nature. The Personal Data Law expressly states that every individual has the right to be aware (by legal means) that his personal data is registered, as well as the purpose of registering it. Further, the content of the collected personal data must be appropriate and limited to achieving the purpose of its collection (which the individual is aware of).

Further to the above, the Personal Data Protection Law provides that when assessing the reliability of an electronic transaction, including a digital or electronic evidence, several items must be considered, including the method of creating, storing, or communicating an electronic record and the possibility of amending the same, as well as the method of maintaining the integrity of information and the method of identifying the originator. In other words, the Court handling the relevant claim will consider the steps taken for obtaining/creating a digital evidence that is provided to it, in order to determine whether to accept it.

In conclusion, although digital evidence are currently not commonly used or provided as evidence to Courts, we expect to see more reliance from litigation parties on electronic and digital evidence as well as more acceptance from Courts to consider them. When creating digital and electronic evidence, they must be created with the consent of the concerned parties, maintained with integrity and in a way whereby the originator can be identified, or else, such digital or electronic evidence would be at risk of not being acceptable to the Court.

***For further information, please contact [Lina Samaha](#).***