Date: 18th Nov 2022

REF: TRAI Consultation Paper on Leveraging Artificial Intelligence and Big Data in Telecommunication Sector dated 05 August 2022

To
Shri Asit Kadayan, Advisor (QoS) Telecom Regulatory Authority of India,

(Through email: advqos@trai.gov.in)

The following inputs/comments/counter comments regarding AI & BD in telecom sector:

After observing a long consultation paper & 20 responses, the following points to be reviewed to understand the **reality**:

1) Do we know what the actual tele-density in our Nation is?
   We are just arriving the tele-density based on mere figures viz., population and number of connections, without considering multiple telephones/mobiles/broadbands having by a single person from multiple TSPs/ISPs.
2) Do we have OSHA standards for persons working on telecom towers/telecom environment?
   Department of Labour issued (long back) guidelines to all sectors to formulate OSHA standards basing on the working nature in their department/sector. By this time lakhs of telecom towers are in place without having OSHA standards for the persons working on telecom towers.
3) Do you have any audit system on all the APPs available for mobile users? May escape by saying that subject belongs to IT and not Telecom.
   The line between Telecom & IT is to be properly dealt and the confusion among authorities should not be a weapon to anti-social activists.
4) KYC is a crucial step before providing any service. Is it is implemented in true spirit?
   For the past many years, providing tele-services based on the documents submitted. No entity is verifying KYC physically. At least no physical check on the address of the person/entity to whom they are providing tele-services. Now, other entities are providing their services basing on the OTP sent on that mobile number assuming that TSPs have completed KYC. This is reason for multiplication of mistakes and leading to a chain reaction of cyber frauds/frauds/crimes in the society. The cost of physical KYC verification is definitely not greater than the loss happened due to cyber frauds/crimes.

What is in our hands is to be handled systematically, before going forward.

Sharing of information/details between any entities, in any form/technology for business purpose is not acceptable. Whatever may be the technology we name/call it, the details/information of a person is to be kept within the entity and not to be shared with other entities (even it may be programmed algorithms), except law & enforcement/Government agencies that too limited to the particular incident.

TSP: Tele-Service Provider, **ISP:** Internet Service Provider, **OSHA**: Occupational Safety and Health Administration, **APP:** Applications, **IT:** Information Technology, **KYC**: Know Your Customer, **OTP:** One Time Password/code

Regards
Vas KSS